# PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-169681**

(43)Date of publication of application : **14.06.2002**

(51)Int.Cl. G06F 3/12
B41J 5/30
B41J 29/00
B41J 29/38
G06F 12/14
G06F 15/00
G09C 1/00
H04N 1/44

(21)Application number : **2001-215195**

(22)Date of filing : **16.07.2001**

(71)Applicant : **TRUSTCOPY PTE LTD**

(72)Inventor : **WU JIAN KANG**
**ZHU BAOSHI**
**ZHU QUNYING**
**HUANG SHENG**

(30)Priority

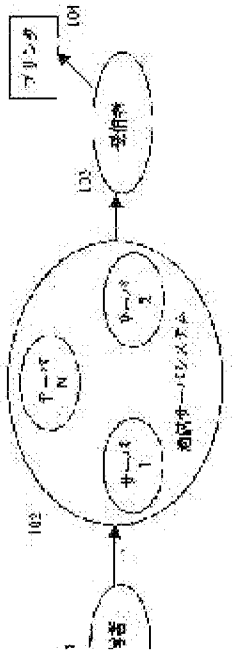
Priority number : **2000 5827** Priority date : **11.10.2000** Priority country : **SG**

## (54) PROTECTION OF SAFETY OF SECRET AND/OR REMOTE PRINTING OF CERTIFICATED DOCUMENT

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method and apparatus capable of printing certificated documents at remote sites and of controlling the printing.

SOLUTION: A method of remote printing of documents through a network comprises a step (a) to receive the documents transmitted from a sender 101 at a server 102, a step (b) to transfer the documents to a recipient 103 from the server 102, a step (c) to certificate the documents before transferring to the recipient 103 and a step (d) of receiving by the server 102 of instructions relating to printing control of a printer 104 from the sender 101 and of performing of controlling by the server



102 at a side of the recipient 103.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－169681
（P2002－169681A）
(43)公開日　平成14年６月14日(2002.6.14)

| (51)Int.Cl.[7] | 識別記号 | ＦＩ | | テーマコード（参考） |
|---|---|---|---|---|
| Ｇ０６Ｆ　3/12 | | Ｃ０６Ｆ　3/12 | Ｄ | ２Ｃ０６１ |
| Ｂ４１Ｊ　5/30 | | Ｂ４１Ｊ　5/30 | Ｚ | ２Ｃ０８７ |
| 29/00 | | 29/38 | Ｚ | ５Ｂ０１７ |
| 29/38 | | Ｇ０６Ｆ　12/14 | ３２０Ａ | ５Ｂ０２１ |
| Ｇ０６Ｆ　12/14 | ３２０ | | ３２０Ｅ | ５Ｂ０８５ |

審査請求　未請求　請求項の数72　ＯＬ　（全 31 頁）　最終頁に続く

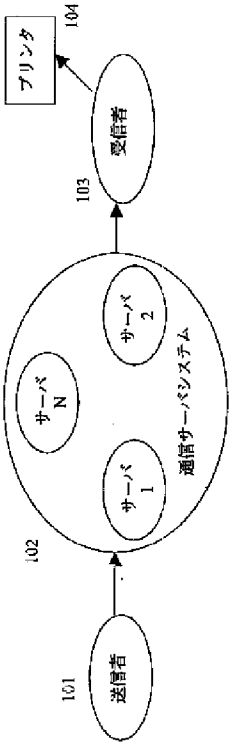
(21)出願番号　特願2001－215195(P2001－215195)
(22)出願日　平成13年７月16日(2001.7.16)
(31)優先権主張番号　２００００５８２７－１
(32)優先日　平成12年10月11日(2000.10.11)
(33)優先権主張国　シンガポール（ＳＧ）

(71)出願人　501130084
トラストコピー・ピーティーイー・リミテッド
シンガポール国、119631　ヘン・ムイ・ケン・テラス　21、ケント・リッジ・デジタル・ラブス内
(72)発明者　ジャン・カン・ウー
シンガポール国、600051　テパン・ガーデンズ・ロード、　ナンバー　06－565、ビーエルケー　51
(74)代理人　100058479
弁理士　鈴江　武彦　（外４名）

最終頁に続く

(54)【発明の名称】　秘密の安全の保護および、または認証された文書の遠隔印刷

(57)【要約】
【課題】　本発明は、認証された文書を遠隔位置で印刷し、その印刷を制御することができる方法および装置を提供することことを目的とする。
【解決手段】ネットワークを使用して文書の遠隔印刷を行う方法であって、（ａ）送信者101から送信された文書をサーバ102で受信し、（ｂ）サーバ102が文書を受信者103に転送し、（ｃ）文書が受信者103に転送される前に認証され、（ｄ）サーバ102が送信者101からプリンタ104の印刷制御に関する命令を受信し、サーバ102がこれらの制御を受信者103側で実施するステップを含んでいることを特徴とする。



【特許請求の範囲】
【請求項１】　（ａ）送信者から送信された文書をサーバで受信し、
（ｂ）サーバが文書を受信者に転送し、
（ｃ）文書が受信者に転送される前に認証され、
（ｄ）サーバが送信者から印刷制御に関する命令を受信し、サーバがこれらの制御を受信者側で実施するステップを含んでいるネットワークの使用による文書の遠隔印刷方法。
【請求項２】　（ｄ）送信者が文書をサーバに送信して、そのサーバがその文書を受信者に転送できるようにし、
（ｅ）文書が送信者によってサーバに送信される前に認証され、
（ｆ）文書の印刷を制御するための命令をサーバに送信して、サーバが受信者側でこれらの制御を実行することを可能にするステップを含んでいるネットワークの使用による文書の遠隔印刷方法。
【請求項３】　（ｃ）受信者が、認証された文書を送信者から受信したサーバから認証された文書を受信し、
（ｄ）送信者から印刷制御を受信したサーバが、受信者側で印刷制御を実行するステップを含んでいるネットワークの使用により遠隔的に受信された認証された文書の印刷方法。
【請求項４】　印刷制御は、印刷された文書が送信者により送信された文書内容と正確に同じ内容を有していることを確実にする請求項１乃至３のいずれか１項記載の方法。
【請求項５】　印刷制御は、偽造防止制御を含んでいる請求項１乃至４のいずれか１項記載の方法。
【請求項６】　印刷制御は、コピー防止制御を含んでいる請求項１乃至５のいずれか１項記載の方法。
【請求項７】　印刷制御は、印刷されるべき文書のコピー数に関する制御を含んでいる請求項１乃至６のいずれか１項記載の方法。
【請求項８】　受信者はプリンタを有し、サーバが文書の印刷のためにプリンタに印刷制御を行う請求項１乃至７のいずれか１項記載の方法。
【請求項９】　サーバは、秘密が安全に保護された文書が送信者からサーバを通って受信者に配信されることを可能にしている請求項１乃至８のいずれか１項記載の方法。
【請求項１０】　サーバは、送信者が印刷制御において信頼できる代行業者である請求項１乃至９のいずれか１項記載の方法。
【請求項１１】　サーバは、文書検証サービスにおいて信頼できる第３のパーティである請求項１乃至１０のいずれか１項記載の方法。
【請求項１２】　サーバは文書のハッシュと、文書の少なくとも１つの内容特徴とを記憶しており、それらを文書検証のために使用する請求項１１記載の方法。
【請求項１３】　秘密が安全に保護された文書配信および印刷制御は、
（ａ）文書自身、
（ｂ）手書き署名、
（ｃ）デジタル署名、
（ｄ）光学的透かし模様、
（ｅ）文書の内容特徴、
（ｆ）使用制御および監査証跡、
（ｇ）送信者のシール、
（ｈ）満期日からなるグループからの１以上のものを含む信頼できる文書構造に基づいている請求項１１または１２記載の方法。
【請求項１４】　送信者は文書についての許可をする請求項１１乃至１３のいずれか１項記載の方法。
【請求項１５】　公開キーインフラストラクチャを使用して、文書の配信時の拒否防止、プライバシー、および秘密の安全の保護を実行する請求項１乃至１４のいずれか１項記載の方法。
【請求項１６】　デジタル署名が文書に適用され、デジタル署名は送信者、サーバ、受信者からなるグループから選択された１以上のもののデジタル署名である請求項１３または１４記載の方法。
【請求項１７】　送信者はサーバに登録された後、文書を送信することが可能にされる請求項１乃至１６のいずれか１項記載の方法。
【請求項１８】　受信者はサーバに登録された後、文書を受信することが可能にされる請求項１乃至１７のいずれか１項記載の方法。
【請求項１９】　文書ハッシュおよび内容特徴は検証用の文書と共に送信され、文書のハッシュおよび内容特徴は将来の検証のためにサーバ中に保持されている請求項１４乃至１８のいずれか１項記載の方法。
【請求項２０】　秘密の安全の保護されたソケット層プロトコルによって提供された安全文書転送チャンネルが使用され、送信者および受信者はユーザアイデンティティおよび少なくとも１つのパスワードを使用することによって認証される請求項１乃至１３のいずれか１項記載の方法。
【請求項２１】　秘密の安全の保護された文書配信のために暗号化技術を使用する請求項１乃至１３のいずれか１項記載の方法。
【請求項２２】　文書を解読するためのキーは、ｅメール、電話、郵便、クーリエおよび個人配送からなるグループから選択された伝達手段によって受信者に直接送られる請求項２１記載の方法。
【請求項２３】　印刷される文書は、光学的透かし模様、特別のインク、特別の紙および特別の印刷材料からなるグループから選択された認証手段を使用して許可されていないコピーおよび偽造から保護されている請求項

１乃至２２のいずれか１項記載の方法。
【請求項２４】　光学的透かし模様は、模造防止層を有している請求項２３記載の方法。
【請求項２５】　模造防止層の性能を高レベルにするようなプリンタの較正を含んでいる請求項２４記載の方法。
【請求項２６】　較正は、人間の介入なしに印刷言語を使用して行われる請求項２５記載の方法。
【請求項２７】　プリンタは、印刷制御プロセスにおいて秘密の安全が保護されている請求項８乃至２６のいずれか１項記載の方法。
【請求項２８】　プリンタは秘密の安全が保護されたメモリ、秘密の安全が保護された中央処理装置および秘密の安全が保護されたクロックを含んでおり、秘密の安全が保護されたメモリは専用キーを記憶するために使用され、秘密の安全が保護された中央処理装置はランタイムアタックを阻止するために使用され、秘密の安全が保護されたクロックは時間をキープするために使用される請求項２７記載の方法。
【請求項２９】　プリンタおよびサーバシステムは、互いに認証するために秘密の安全の保護されたハンドシェークを行い、プリンタの公開キー対またはプリンタの対称キーからなるグループから選択された１以上のものを使用する請求項２７記載の方法。
【請求項３０】　サーバは暗号化された文書ハッシュ、光学的透かし模様および印刷命令をプリンタに送信する請求項２７記載の方法。
【請求項３１】　プリンタは、文書をクライアントソフトウェアから受信し、その文書を解読し、印刷する前にハッシュおよび時間スタンプによりその文書を検証し、印刷中光学的透かし模様を追加する請求項３０記載の方法。
【請求項３２】　文書は印刷直後に秘密の安全が保護されたメモリから消去される請求項２８乃至３１のいずれか１項記載の方法。
【請求項３３】　サーバにおいて監査証跡記録を生成するステップをさらに含んでいる請求項８乃至３２のいずれか１項記載の方法。
【請求項３４】　クライアントソフトウェアが、文書を印刷するために受信者のマシンにダウンロードされる請求項１乃至２６のいずれか１項記載の方法。
【請求項３５】　受信者は、クライアントソフトウェアに対するアタックを最小にする印刷制御プロセスにおいて信頼できるものである請求項３４記載の方法。
【請求項３６】　サーバはクライアントソフトウェアによってプリンタと通信して、プリンタ製造番号およびインターネットプロトコルアドレスを検証し、プリンタの状態をチェックし、プリンタの制御パネルをロックし、必要なプリンタ設定を全て行い、文書およびその文書を印刷するための命令をプリンタに送信し、印刷プロセスが完了した後にプリンタ設定をリセットし、サーバにおいて監査証跡記録を生成する請求項３５記載の方法。
【請求項３７】　シールは、手書き署名およびシールと、印刷された全てのコピーに共通している共通シールおよび印刷された各コピーに特有である特有のシールを含むシールからなるグループから選択された１以上のものを含んでいる請求項１３記載の方法。
【請求項３８】　クライアントソフトウェアは基本部分および感応部分を有しており、感応部分は基本部分よりアタックを受け易く、基本部分は受信者がサーバに登録されたときにその受信者に送られ、感応部分は文書を印刷するために受信者のマシンにダウンロードされ、感応部分をアタックから保護するために印刷の完了時に受信者のマシンから消去される請求項３４乃至３６のいずれか１項記載の方法。
【請求項３９】　暗号化された形態の感応部分は、受信者がサーバにより登録されたときにその受信者に送信され、そのサーバが解読キーを管理し、感応部分は要求されたときに解読される請求項３８記載の方法。
【請求項４０】　受信者に対する基本部分の送信と同時に、あるいはその前に、基本部分のハッシュの結果が出されてもよく、このハッシュ結果はサーバに記憶され、また、受信者が文書の印刷を要求した場合、基本部分の第２のハッシュ結果が出され、印刷がサーバにより許可される前にハッシュ結果と比較される請求項３８または３９記載の方法。
【請求項４１】　感応部分の構成要素の実行に対する実行時間がサーバ中に記録され、文書の印刷中に構成要素の実行に要した時間と比較され、この要した時間が実行時間より著しく長い場合には印刷が終了される請求項３８乃至４０のいずれか１項記載の方法。
【請求項４２】　印刷制御は、受信者による文書の印刷に対するリクエストに応答して実施される請求項１乃至４３のいずれか１項記載の方法。
【請求項４３】　印刷制御はオフラインで実行され、サーバはその印刷プロセスに関与しない請求項１乃至２６のいずれか１項記載の方法。
【請求項４４】　サーバの代りに活動するハードウェア装置が受信者側に設けられている請求項４３記載の方法。
【請求項４５】　ハードウェア装置は文書の印刷を制御し、秘密の安全が保護されたメモリ、読出し後消去されるメモリ、オンチッププログラムを備えた中央処理装置、およびインターフェースを含んでおり、ハードウェア装置はサーバに登録される請求項４４記載の方法。
【請求項４６】　マシンはプリンタを含んでおり、ハードウェア装置はプリンタと一体であり、そのプリンタがサーバに登録される請求項４３または４４記載の方法。
【請求項４７】　秘密の安全が保護されたメモリはアクセス可能なメモリと、内部使用のための制御されたメモ

リとを有しており、アクセス可能なメモリは、ユーザのパスワードが入力されて検証された場合にのみアクセスされることができ、このアクセスはそのユーザに関連したアクセス可能なメモリのブロックに対してのみ行われ、制御されたメモリは複数のブロックに分割され、各ユーザに対して１つの制御されたメモリブロックが存在する請求項４５記載の方法。

【請求項４８】　制御されたメモリは秘密キー、製造番号、ユーザの専用キーおよび受信者のＩＤキーを記憶する請求項４７記載の方法。

【請求項４９】　制御は、受信者が文書を印刷することに対するライセンスの発行を含んでいてもよく、そのライセンスは印刷を許可された文書のコピーの数を含んでいる請求項１３乃至４８のいずれか１項記載の方法。

【請求項５０】　各ライセンスは特有のシールを暗号化するために使用されるライセンスキーを有しており、そのライセンスキーは暗号化された形態でサーバによって受信者に送信され、ハードウェア装置にインストールされる請求項４９記載の方法。

【請求項５１】　サーバはライセンスキーの数を増加することが可能であり、サーバは新しいライセンスキーセットおよび新しいトップアップキーを生成し、新しいライセンスキーセットおよび新しいトップアップキーは、サーバによって受信者に送信されてハードウェア装置にインストールされる前に、前のトップアップキーにより暗号化される請求項５０記載の方法。

【請求項５２】　各ライセンスは、その後はもはやそのライセンスを使用して文書を印刷することのできない満期日を含んでいる請求項４９乃至５１のいずれか１項記載の方法。

【請求項５３】　新しいライセンスキーセットは文書とは別々に送信される請求項５１記載の方法。

【請求項５４】　新しいライセンスキーセットは文書と一緒に送信される請求項５１記載の方法。

【請求項５５】　送信者が文書を送信する前に、送信者の共通のシール、送信に対する時間スタンプ、および満期日が第１のセッションキーにより暗号化され、暗号化された結果を生成する請求項４９乃至５２のいずれか１項記載の方法。

【請求項５６】　暗号化された結果および文書は第２のセッションキーにより暗号化され、第２の暗号化された結果を生成する請求項５５記載の方法。

【請求項５７】　第２の暗号化された結果にはデータの完全性をチェックする手段を提供するハッシュ結果が含まれている請求項５６記載の方法。

【請求項５８】　印刷制御は、文書を印刷するのではなく、見るためのものであることができ、見るためにライセンスは必要ない請求項４９乃至５７のいずれか１項記載の方法。

【請求項５９】　満期日は、文書の印刷が許可される前にチェックされ、満期日が過ぎていた場合、文書の印刷は許可されない請求項１３乃至５８のいずれか１項記載の方法。

【請求項６０】　送信者およびサーバは同一であり、送信者の全ての機能はサーバによって行われる請求項１乃至５９のいずれか１項記載の方法。

【請求項６１】　送信者は、秘密の安全が保護されたハードウェア装置を複数の受信者のそれぞれに供給する許可の権限を有する者であり、文書とライセンスキーがネットワークによってその各受信者に送信され、各受信者は文書を印刷するために秘密の安全が保護されたハードウェア装置を使用し、その文書は受信者によってその受信者の顧客に対して印刷された文書または電子文書として送られ、秘密の安全が保護されたハードウェア装置が電子文書の送信を制御し、監査証跡を生成して、新しいライセンスキーがトップアップされた場合は常にその監査証跡を許可の権限のある者に送信する請求項６０記載の方法。

【請求項６２】　文書は、郵便切手、税金明細記入請求書および、または税金領収書からなるグループから選択される請求項６１記載の方法。

【請求項６３】　郵便切手、税金明細記入請求書および、または税金領収書の各金額が監査証跡中に含まれている請求項６２記載の方法。

【請求項６４】　許可の権限のある者は、監査証跡中に含まれる金額に基づいて支払うべき税金を決定する請求項６３記載の方法。

【請求項６５】　印刷制御を受信者側で実施するために秘密の安全が保護されたソフトウェアプログラムが提供される請求項４３乃至６４のいずれか１項記載の方法。

【請求項６６】　ソフトウェアプログラムはソフトウェアのアタックの阻止を支援するために分散方式で構成されている請求項６５記載の方法。

【請求項６７】　ライセンスキーおよび監査証跡用の秘密の安全の保護されたメモリは分散方式で構成されている請求項６６記載の方法。

【請求項６８】　ユーザのマシンによる少なくとも１つの文書の印刷の制御を可能にするためにそのマシンにより使用されるハードウェア装置において、
秘密の安全が保護されたメモリ、読出し後消去されるメモリ、オンチッププログラムを備えた中央処理装置、およびインターフェースを含んでいるハードウェア装置。

【請求項６９】　秘密の安全の保護されたメモリはアクセス可能なメモリと、制御されたメモリとを有しており、アクセス可能なメモリはユーザのパスワードが入力されて検証された場合にのみアクセスされることができ、このアクセスはそのユーザに関連したアクセス可能なメモリのブロックに対してのみ行われ、制御されたメモリは複数のブロックに分割され、各ユーザに対して１つの制御されたメモリブロックが存在する請求項６８記

載のハードウェア装置。
【請求項７０】　制御されたメモリは、秘密キー、製造番号、ユーザの専用キーおよび受信者のＩＤキーを記憶する請求項６９記載のハードウェア装置。
【請求項７１】　ハードウェア装置は、秘密の安全の保護されたソフトウェアプログラムとして構成されている請求項６８乃至７０のいずれか１項記載のハードウェア装置。
【請求項７２】　秘密の安全の保護されたソフトウェアプログラムは、ソフトウェアのアタックの阻止を支援するために分散方式で構成されている請求項７１記載のハードウェア装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、安全（秘密の保護）および、または認証された文書の印刷を制御する方法および装置に関し、とくに、印刷プロセスに対する制御を含むこのような方法および装置に関するが、それに限定されるものではない。
【０００２】
【従来の技術】この明細書全体を通して、“文書”と言った場合には電子または印刷された形態の文書がそれに含まれるものとする。
【０００３】この明細書全体を通して、“認証”と言った場合には安全保護が含まれ、反対に“安全保護”と言った場合には認証が含まれる。
【０００４】この明細書全体を通して、“マシン”と言った場合には、デスクトップコンピュータ、ラップトップコンピュータ、ノートブックコンピュータ、または任意の他の適切な形態のコンピュータがそれに含まれるものとする。
【０００５】この明細書全体を通して、“印刷”と言った場合には、印刷、表示、リスニング、保存、電子送信、転送および類似の機能を含む受信者による文書の全ての形態の処理がそれに含まれるものとする。
【０００６】通常、業務を行なうために、また事務管理のために紙の文書が使用されている。ペーパーレスオフィスが繰返し予言されてきたにもかかわらず、デジタル世代になってもオフィス内における紙の使用は増加している。この主な理由は信頼性である。ある文書が権限を有する人物によって署名されたとき、彼等の署名によりそれが認証される。署名が記されている場合は常に、あるいは署名が記されているものは全て、その文書が本物であるというある程度の確信をもって処理されることができる。オリジナル文書の数が厳密に制御され、知られることにより、秘密保護の安全性が確保される。
【０００７】米国特許第 6,091,507号明細書には、ネットワークを介して文書を印刷する方法および装置が記載されている。その明細書にはネットワークプロトコル、送信フォーマット、およびラスターイメージプロセッサを有するホストコンピュータからプリンタへのラスターデータの高速送信を容易にするハードウェアインターフェースが示されている。明らかに、安全保護された、信頼できる、あるいは認証された文書にとって重要ないくつかの関連した問題の解決方法は記載されていない。
【０００８】米国特許第 5,983,065号明細書には、安全保護された文書を印刷する方法が記載されている。この方法はオリジナル文書を印刷するためにアクセス制御された電子印刷マシンを使用する。それによって形成された印刷されるイメージは可視光の中で認識可能であり、少なくとも１つの光活性化合物を含むマーキング材料（液体インクおよび、または乾燥トナー）から生成される。印刷されたオリジナル文書イメージは、通常のコピー機またはスキャナでコピーまたはスキャンされることはできない。それは特殊印刷材料を使用している。
【０００９】米国特許第 5,917,996号明細書には、安全確保された背景を覆う、不正操作を防止（ｔａｍｐｅｒ－ｒｅｓｉｓｔａｎｔ）する複合的な電子形態の文字を使用して不正操作防止形態を印刷する方法が開示されている。
【００１０】米国特許第 6,085,181号明細書には、ネットワーク上でメーターサーバとして動作する独立型メータ用の郵便料金メーターシステムが記載されている。プリンタモジュールは、郵便セキュリティ装置（ＰＳＤ）と接続されたそのネットワーク上のクライアントプリンタモジュールとして動作する。このＰＳＤには、特有の識別子、郵便料金記憶装置およびデジタル署名発生器が含まれる。クライアントプリンタはＰＳＤからの郵便料金支払いの証拠を、ローカルクライアントプリンタモジュールを介してリクエストし、郵便料金メータートランザクションを終了する。郵便料金支払いの証拠には、郵便料金支払いの証拠に対する各リクエストに対応したデジタル署名が含まれる。この特許明細書は、郵便料金の使用制御に関するものである。
【００１１】
【発明が解決しようとする課題】従来技術には、文書に対してなされたコピーの数の制御と、およびその文書の認証の制御という２つの非常に重要な問題の解決方法を開示したものはない。
【００１２】本発明の主な目的は、認証された文書を遠隔位置で印刷し、その印刷を制御することができる方法および装置を提供することである。
【００１３】
【課題を解決するための手段】上記およびその他目的を考慮して、本発明は、ネットワークを使用することによって文書を遠隔印刷する方法を提供し、この方法は、
（ａ）送信者から送られた文書をサーバで受信し、
（ｂ）サーバがこの文書を受信者に転送し、（ｃ）その文書が受信者に転送される前に認証され、（ｄ）サーバが印刷制御に関する命令を送信者から受信し、これらの

制御を受信者側で実施するステップを含んでいる。

【００１４】本発明はまた、ネットワークを使用することによって文書を遠隔印刷する方法を提供し、この方法は（ａ）送信者が文書をサーバに送信し、それによってサーバが文書を受信者に転送することが可能になり、（ｂ）文書がサーバに送信される前に送信者によって認証され、（ｃ）文書の印刷を制御するための命令をサーバに送信し、それによってサーバが受信者側でこれらの制御を実施することが可能になるステップを含んでいる。

【００１５】別の形態において、本発明は、ネットワークの使用により遠隔的に受信された認証された文書を印刷する方法を提供し、この方法は、（ａ）受信者が認証された文書をサーバから受信し、そのサーバは認証された文書を送信者からすでに受信しており、（ｂ）サーバが印刷の制御を受信者側で行い、そのサーバは印刷制御を送信者からすでに受信しているステップを含んでいる。

【００１６】印刷制御は、印刷された文書が、送信者によって送られた文書内容と正確に同じ内容を有し、および、または偽造防止制御および、またはコピー防止制御および、または印刷されるべき文書のコピーの数に関する制御を確実に有するようにされることが好ましい。

【００１７】受信側装置はプリンタを含み、送信側装置が文書を印刷するためにそのプリンタに印刷制御信号を配信してもよい。サーバは、安全保護された文書が送信者からサーバを通って受信者に配信されることを可能にすることが好ましく、また、サーバは送信者が印刷制御において信頼できる代行業者であってもよい。サーバはまた文書検証に関して信頼できる第３のパーティであってもよい。サーバはこれを行うために、そのサーバに記憶されている文書のハッシュおよび内容特徴を使用してもよい。安全保護された文書の配信および印刷制御は、（ａ）文書自身、（ｂ）手書きによる署名、（ｃ）デジタル署名、（ｄ）光学的透かし模様（ｅ）文書の内容特徴、（ｆ）使用制御および監査証跡、（ｇ）送信者のシール（証印）、および（ｈ）満期日の１以上のものを含む信頼できる文書構造に基づいてもよい。

【００１８】送信者は、文書を認可する者であってもよい。この方法は、公開キーインフラストラクチャを使用して文書の配信時の拒絶防止、プライバシーおよび機密保護および安全保護を実現することができる。

【００１９】デジタル署名が文書に適用されてもよく、デジタル署名は送信者、サーバおよび、または受信者の署名である。送信者および受信者は、送信および受信をそれぞれ行う前にサーバに登録されることが好ましい。文書ハッシュおよびその内容特徴は正当性の検査のために文書と共に送信され、その文書のハッシュと内容特徴が将来的な検証のためにサーバに保持されることができる。

【００２０】この方法は安全保護ソケット層プロトコルによって提供される安全保護された文書転送チャンネルを使用でき、送信者および受信者の認証はユーザアイデンティティおよび少なくとも１つのパスワードによってなされてもよい。

【００２１】この方法はまた、安全保護された文書配信のために暗号技術を使用することができる。したがって、文書を解読するためのキーは、ｅメール、電話、郵便、クーリエおよび個人配送からなるグループから選択された伝達手段によって受信者に直接送られることができる。

【００２２】印刷された文書は、光学的透かし模様、特殊インク、特殊な紙および特殊な印刷材料からなるグループから選択された認証手段を使用して、許可されていないコピーおよび偽造から保護されることができる。

【００２３】光学的透かし模様は、模造防止層を有していてもよい。模造防止層の性能を高レベルにするようにプリンタが較正されてもよい。較正は人間の介入なしに印刷言語を使用して行われてもよい。また、プリンタは、印刷制御プロセスにおいて安全保護されてもよく、安全保護されたメモリ、安全保護された中央処理装置および安全保護されたクロックを含んでいてもよい。安全保護されたメモリは専用キーを記憶するために使用され、安全保護中央処理装置はランタイムアタックを阻止するために使用され、また、安全保護クロックは時間を合わせておくために使用されることができる。プリンタおよびサーバは、互いに認証するために安全保護されたハンドシェークを行い、プリンタの公開キー対または対称キーを使用することが好ましい。

【００２４】サーバは暗号化された文書ハッシュ、光学的透かし模様および印刷命令をプリンタに送信することができる。

【００２５】プリンタは、文書をクライアントソフトウェアから受信し、その文書を解読し、印刷する前にハッシュおよび時間スタンプによりその文書を検証し、印刷中光学的透かし模様を追加することができる。

【００２６】プリンタは印刷した直後に文書を消去することが好ましく、監査証跡記録がサーバにおいて生成される。

【００２７】受信者は印刷制御プロセスにおいて信頼されることができる。この場合、サーバはクライアントソフトウェアによってプリンタと通信し、プリンタ製造番号およびインターネットプロトコルアドレスを検証し、プリンタの状態をチェックし、プリンタの制御パネルをロックし、必要なプリンタ設定を全て行い、印刷するために文書をプリンタに送信し、印刷プロセス終了後にプリンタ設定をリセットし、サーバにおいて監査証跡記録を生成することができる。

【００２８】シール（証印）は、手書きによる署名とシール、印刷された全てのコピーに共通している共通シー

ルを含むシール、および印刷された各コピーに特有の特有のシールからなるグループから選択された１以上のものを含むことができる。

【００２９】基本部分および感応部分を有するクライアントソフトウェアが含まれることが可能であり、その感応部分は基本部分よりアタックを受け易く、基本部分は、受信者がサーバに登録されたときにその受信者に送信される。感応部分は文書を印刷するために受信者のマシンにダウンロードされ、感応部分をアタックから保護するために印刷の終了時に受信者のマシンから消去される。暗号化された形態の感応部分は、受信者がサーバに登録されたときにその受信者に送信されることが好ましく、そのサーバが解読キーを管理し、感応部分は要求されたときに解読される。

【００３０】受信者に対する基本部分の送信と同時に、あるいはその前に、基本部分のハッシュの結果が採取されてもよく、このハッシュ結果はサーバに記憶され、また、受信者が文書の印刷を要求した場合には、基本部分の第２のハッシュ結果が採取され、印刷がサーバにより許可される前にハッシュ結果と比較される。

【００３１】クライアントソフトウェアは、受信者のハードウェア装置に記憶されていてもよい。

【００３２】その代わりに、あるいはそれに加えて、感応部分の構成要素の実行するための実行時間がサーバに記録され、文書の印刷中に構成要素を実行するのに要した時間と比較されてもよく、この要した時間が実行時間より著しく長い場合には印刷が終了される。

【００３３】印刷制御は、受信者による文書の印刷に対するリクエストに応答して実施されることが好ましい。印刷制御はまた、オフラインで実行されてもよく、サーバはその印刷プロセスに関与しない。その場合には、受信機で印刷制御を実施するためにサーバおよび、または安全保護されたソフトウェアプログラムの代りに活動するハードウェア装置が受信者側に設けられることができる。ソフトウェアプログラムは、ソフトウェアアタックの阻止を支援するために分散（ｄｉｓｔｒｉｂｕｔｅｄ）方式で実施されることが好ましい。

【００３４】送信者およびサーバは同じであってもよく、その場合サーバは送信者の機能の全てを行う。

【００３５】ハードウェア装置は文書の印刷を制御するためのものであってもよく、安全保護されたメモリ、読出し後消去されるメモリ、オンチッププログラムを備えた中央処理装置、およびインターフェースを含み、ハードウェア装置はサーバに登録される。マシンにプリンタが含まれてもよく、ハードウェア装置がプリンタと一体であり、そのプリンタがサーバに登録されてもよい。

【００３６】安全保護されたメモリはアクセス可能なメモリと、内部使用のための制御されたメモリとを有していてもよく、アクセス可能なメモリは、ユーザのパスワードが入力されて検証された場合にのみアクセスされることができ、このアクセスはそのユーザに関連したアクセス可能なメモリのブロックに対してのみ行われ、制御されたメモリは複数のブロックに分割され、各ユーザに対して１つの制御されたメモリブロックが存在し、また制御されたメモリは秘密キー、製造番号、ユーザの専用キーおよび受信者のＩＤキーを記憶するためのものである。

【００３７】制御は受信者が文書を印刷することに対するライセンスの発行を含んでいてもよく、そのライセンスは印刷を許可された文書のコピーの数を含んでいる。各ライセンスは、特有のシールを暗号化するために使用されるライセンスキーを有していることが好ましく、そのライセンスキーは暗号化された形態でサーバによって受信者に送信され、ハードウェア装置にインストールされる。サーバはライセンスキーの数を増加することが可能であってもよく、サーバは新しいライセンスキーセットおよび新しいトップアップキーを生成し、これらの新しいライセンスキーセットおよび新しいトップアップキーは、サーバによって受信者に送信されてハードウェア装置にインストールされる前に、前のトップアップキーによって暗号化される。

【００３８】各ライセンスは、もはやそのライセンスを使用して文書を印刷することのできない満期日を含んでいてもよい。新しいライセンスキーセットが文書と別々に、あるいは一緒に送られてもよい。

【００３９】送信者が文書を送信する前に、送信者の共通シール、送信に対する時間スタンプ、および満期日が第１のセッションキーにより暗号化され、暗号化された結果を生成してもよい。その後、暗号化された結果および文書は第２のセッションキーにより暗号化され、第２の暗号化された結果を生成してもよく、この第２の暗号化された結果にはデータの完全性をチェックする手段を提供するハッシュ結果が含まれている。

【００４０】印刷制御は、文書を印刷するのではなく見るためのものであってもよく、見るためにライセンスは必要ない。満期日は文書の印刷が許可される前にチェックされることが好ましく、満期日が過ぎていた場合、文書の印刷は許可されない。

【００４１】送信者は、安全保護されたハードウェア装置を複数の受信者のそれぞれに供給する権限を有する者であってもよく、文書とライセンスキーがネットワークによってその各受信者に送信され、各受信者は文書を印刷するために安全保護されたハードウェア装置を使用し、その文書は受信者によってその受信者のクライアントに対して印刷された文書または電子文書として送られ、安全保護されたハードウェア装置が電子文書の送信を制御し、監査証跡を生成して、新しいライセンスキーがトップアップされた場合は常に監査証跡を前記の権限を有する者に送信する。

【００４２】文書は、郵便切手、税金明細記入請求書お

よび、または税金領収書であってもよく、各金額が監査証跡中に含まれる。権限を有する者は、監査証跡中に含まれる金額に基づいて支払うべき税金を決定してもよい。

【００４３】別の形態において、本発明はユーザのマシンにより使用されるハードウェア装置を提供し、それによってそのマシンによる少なくとも１つの文書の印刷の制御を可能にし、そのハードウェア装置が安全保護されたメモリ、読出し後消去するメモリ、オンチッププログラムを備えた中央処理装置、およびインターフェースを含んでいる。

【００４４】安全保護されたメモリはアクセス可能なメモリと、制御されたメモリとを有していてもよく、アクセス可能なメモリは、ユーザのパスワードが入力されて検証された場合にのみアクセスされることができ、このアクセスはそのユーザに関して正当なアクセス可能なメモリのブロックに対してのみ行われ、制御されたメモリは複数のブロックに分割され、各ユーザに対して１つの制御されたメモリブロックが存在する。制御されたメモリは秘密キー、製造番号、ユーザの専用（私設）キーおよび受信者のＩＤキーを記憶するためのものである。ハードウェア装置は安全保護されたソフトウェアプログラムとして実施されてもよく、その安全保護されたソフトウェアプログラムはソフトウェアアタックを阻止することを支援するために分散方式で構成されてもよい。

【００４５】

【発明の実施の形態】本発明を十分に理解し、容易に実施するために、以下本発明の好ましい形態のみを添付図面を参照して非限定的な例示によって説明する。本発明は３つの主な構成要素：サーバシステムが信頼できる第３のパーティの役割を果たす文書転送および印刷の全プロセスと、印刷された文書を認証する手段と、および印刷制御自身とから構成されている。

【００４６】［文書転送および印刷の全プロセス］図１を参照すると、安全保護された遠隔文書印刷システムには４つの主要な構成要素が存在している。文書の送信者は、文書を開始（ｉｎｉｔｉａｔｅ）する権限を与えられた人物でなければならない。通信サーバシステムは、安全で信頼性の高い文書の配信に必要なファシリティを提供する少なくとも１つのサーバから構成されている。それは、送信者および受信者の認証時に信頼できる第３のパーティとして活動し、そのトランザクションは内部公開キーインフラストラクチャ（ＰＫＩ）プロトコルに基づいている。それはまた送信者の代わりの信頼できる代行業者として活動し、その送信者の印刷要求を実施し、印刷プロセスを制御する。印刷プロセスは、通信サーバシステムにより受信者のサイトに存在するソフトウェアを介して制御される。暗号技術を使用する安全保護された文書配信に関してはＩＳＯ／ＣＣＩＴＴ　Ｘ．４００を参照し、ＰＧＰに関しては、たとえば、文献（“Network Security-private communication in a public world,” by C.Kaufman,R.Perlman,and M.Speciner,PTR Prentice Hall,1995）を参照されたい。

【００４７】文書の転送中、その文書の構造は図２に示されているようなものとなり、これによって信頼できる文書になる。文書自身と共に、以下の５つの別のアイテムが含まれている：

・直感的な信頼感を人々に与えるための発行権限者の手書き署名および、またはシール；この手書き署名およびシールは、権限者の認証が成功した場合にのみ文書に付加される。このように手書き署名は有意味である。

・拒絶防止および内容の完全性のための、送信者、受信者およびサーバシステムによる文書のデジタル署名；このデジタル署名は、専用キーにより暗号化された文書ハッシュである。３つのパーティの全てによるデジタル署名は、発信元の否認や受信および配信の拒絶がなされないことを保証する。

・文書上の光学的透かし模様；これは文書の認証を行い、文書をコピーおよび偽造から保護する。

・文書の内容特徴；これは文書全体から抽出される。それは文書の内容を検証し、可能性のある変更の位置をつき止めるために使用される。それは、将来の文書検証のためにサーバシステムに記憶されている。

・使用制御および監査証跡記録；これは、権限者によって使用状態を維持し、またコピー制御の実行状態を決定する。それはサーバシステムによって管理されている。

【００４８】手順には３つの選択肢が存在し、それぞれ異なったセキュリティレベルを有している：

（ａ）ＰＫＩに基づく高セキュリティ手順；それはユーザ認証および拒絶防止のための手段を提供する。

（ｂ）安全保護されたソケット層（ＳＳＬ）プロトコルを使用する安全保護された配信；および

（ｃ）対称的な暗号を使用する安全保護された配信。

【００４９】［ＰＫＩに基づく高セキュリティ手順］

［登録］全てのユーザ（送信者および受信者）は、通信サーバシステムを動作させるサービスセンターに登録する。この登録手順は以下のとおりであるが、それに限定されない：

・ユーザは登録を依頼し、彼等の身分証明、ユーザアイデンティティ（“ＩＤ”）、リクエストされるサービスのタイプ、および公共の証明オーソリティから得られるデジタル証明書（利用可能な場合）を提供する；

・サービスセンターはその後、ユーザ信用証明書を検証し、ユーザプロフィールを生成し、このユーザプロフィールをその登録データベースに記憶する。その後、サービスセンターは登録アイデンティティを発生し、その情報および信頼できるクライアントソフトウェアをユーザに転送する。ユーザがデジタル信用証明書を有しない場合、国内証明オーソリティは以下のステップによってそのユーザにデジタル証明書を供給することになる：国内

証明オーソリティがメッセージ認証コード（“ＭＡＣ”）キーを発生し、それをクライアントソフトウェアおよび登録アイデンティティと一緒にユーザに送信する；ユーザがクライアントソフトウェアを使用してキー対を発生し、証明書に対するリクエストを発生し、ＭＡＣキーを使用してそれを暗号化してサービスセンターに送信する。専用キーはユーザのマシンのハードディスク、フロッピー（登録商標）ディスク、ＣＤＲＯＭ、スマートカードまたは任意の他の適切な手段に記憶されていてもよい；その後、サービスセンターはそのリクエストを検証し、ユーザ証明書に署名して返送する。同時に、サービスセンターは証明書データベース中のユーザ証明書のコピーを預ける；サービスセンターはユーザ証明書の指紋をハードコピー上に印刷し、サービスセンターおよび登録されたユーザの両者がハードコピーに署名する。

【００５０】［文書の送信］送信者が文書を受信者に送信するために、以下のステップが行われる：

・送信者は彼等のログインＩＤ、トークン（存在するならば）およびパスワードを入力することによってサーバシステムにログオンする；

・サーバシステムは送信者のアイデンティティを検証し、その検証が成功した場合に受信者の名前、住所、送信されるべき文書、およびその受信者により印刷されることを許されているコピーの数に対するプロンプトを提供する。リクエストされたＩＤを有する受信者がサービスセンターデーベース上に存在している場合、サーバシステムは公開キー証明書を証明書データベースから抽出し、特有の通し番号を発生し、トランザクションの時間を記録する。トランザクションのプロセス全体に要する時間は無視されることができると仮定する。受信者がサービスセンターに登録していない場合、クライアントソフトウェアはセッションキーを生成し、そのセッションキーを使用してデータを暗号化し、パスワードを使用してセッションキーを暗号化し、別のｅメール、電話またはその他の手段によってパスワードを送信する；

・送信者は受信者の証明書、ＩＤ、およびトランザクションの時間を検証する。その後、送信者のクライアントソフトウェアは送信されるべき文書のハッシュに加えて、通し番号、時間、送信者のＩＤ、および受信者ＩＤを計算し、送信者の専用キーを使用してこれらに署名し、それをサーバシステムに送信する；

・サーバシステムは署名の認証をチェックし、それ自身の署名を生成する；

・送信者はサーバシステムの署名を検証し、それを文書中に組み込む；

・送信者のクライアントソフトウェアはその文書に対して：送信者の手書きの署名、送信者の会社のシールおよび文書の内容特徴を追加し；サーバシステムの証明書を使用して内容特徴およびハッシュを暗号化し、受信者の証明書を使用して情報およびハッシュの残りを暗号化し、それをサーバシステムにアップロードする；

・暗号化された文書を受信すると、サーバシステムはそれを証拠データベースに記憶し、その受信者に通知を送信する。ハッシュおよび内容特徴は、文書認証のために予め定められた期間のあいだサーバ中に記憶されている。

【００５１】［文書の受信］上記のステップに続いて：

・サーバシステムは、文書の利用可能性を受信者に知らせる。文書ＩＤおよび文書の通し番号もまた送信される；

・受信者は受信者ＩＤ、トークン（存在するならば）およびパスワードによりサーバシステムにログオンする；

・サーバシステムは正当性をチェックし、通し番号、時間、送信者ＩＤおよび受信者ＩＤのハッシュを生成する。それはこれらに署名し、署名およびハッシュを受信者に送信する。送信者の検証、暗号化された文書および送信者の署名もまたこの情報と共に送信される；

・その後、受信者は送信者の公開キー証明書の正当性を検査し、文書を解読し、ハッシュを発生し、サーバシステムにより生成されて送信されたハッシュを相互チェックする。それらが一致した場合、検証は成功である。この検証には、サーバシステムによる送信の時間もまた含まれなければならない；

・受信者のクライアントソフトウェアは文書ハッシュ、通し番号、受信者ＩＤ、ならびに送信者ＩＤおよび時間のハッシュの署名を生成し、それをサーバシステムに送信する。これによって、サービスセンターは、その文書の解読が成功したことを完全に確認できる；

・その後、サーバシステムはこの情報を検証し、関連した情報を証拠データベースに記憶する；

・受信者が印刷のリクエストを提起したときに、サーバシステムはクライアントソフトウェアによって受信者サイトにおけるプリンタと通信し、その状態をチェックする。プリンタの準備が整っている場合、サーバシステムは印刷のために文書および光学的透かし模様を送信する。エラーメッセージがなければ印刷は成功である。サーバシステムは全プロセスを記録するために監査証跡を生成する；

・サーバシステムは受信者に承認を送信し、送信者に通知する。

【００５２】［ＳＳＬを使用する安全保護された配信］ＳＳＬ（安全保護されたソケット層）プロトコルは、文献（“Transport Layer Security,”version 1,RFC2246,1999）に記載されているように、２つのパーティ間に安全保護されたチャンネルを提供する。ＳＳＬチャンネルを通る全てのデータ転送は、セッションキーを使用して暗号化される。セッションキーは各接続に対してランダムに発生される。送信ステップは：

・送信者はサーバシステムとの接続を設定し、ＳＳＬセ

ッションキーと安全について協議する。その後、後続する全てのトランザクションは暗号化されたチャンネルを通過する；
・送信者は彼等のログインＩＤおよびパスワードによりシステムにログオンする；
・サーバは送信者のアイデンティティを彼らのログインＩＤおよびパスワードによって検証する；
・その後、送信者はデータ（文書であってもよい）を受信者に送信するリクエストを提起する；
・サーバはそのリクエストを承認し、データを受信するための準備をする；
・送信者はハッシュおよび内容特徴と共にデータを送信する；
・データを受信すると、サーバシステムはそれを証拠データベース中に記憶し、受信者に通知を送る。ハッシュおよび内容特徴は予め定められた期間のあいだサーバに記憶され、将来の認証サービスに使用されることとなる；
・受信者が通知を受信したとき、彼等はクライアントソフトウェアによりサーバとの接続を設定し、ＳＳＬセッションキーと協議する。これに後続する全てのトランザクションは暗号化されたチャンネルを通過する；
・その後、受信者は彼等のログインＩＤおよびパスワードによりシステムにログオンする；
・サーバは受信者のログインＩＤおよびパスワード検証する。正しいと検証された場合、サーバはその受信者にデータを配信する；
・受信者はデータを受信し、サーバに承認を送信する；
・受信者が認証されたコピーを印刷するというリクエストを提起した場合、サーバはハッシュおよび内容特徴により文書を検証し、そのプリンタと通信し、印刷のために文書および光学的透かし模様を送信する。プロセス全体の状態を記録するために監査証跡が生成される。
【００５３】［暗号を使用する安全保護された配信］
・送信者は彼等のログインＩＤおよびパスワードによってサーバにログインする；
・サーバは送信者のログインＩＤおよびパスワードを検証する；
・その後、送信者はデータ（やはり文書であってもよい）を送信するリクエストを提起する；
・サーバはそのリクエストを承認し、データを送信者から受信する準備をする；
・送信者はハッシュおよび内容特徴をデータから生成し、データを暗号化するためのランダムセッションキーを発生する。そのキーおよびハッシュはパスワードを使用して暗号化され、ハッシュおよび内容特徴はサーバシステムの公開キーを使用して暗号化され、その後サーバシステムにアップロードされる；
・サーバシステムは暗号化されたデータ、キー、ハッシュおよび内容特徴を受信し、それらをデータベース中に記憶する；
・その後、送信者は電話、ｅメール、郵便、個人配達またはその他の方法によりパスワードを受信者に通知する；
・受信者が送信者からパスワードを受取ったとき、受信者は彼等のログインＩＤおよびパスワードによりサーバにログインする；
・サーバはそのログインＩＤおよびパスワード検証する。正しいと検証された場合、それは暗号化されたデータ、キーおよびハッシュをその受信者に配信する；
・受信者は暗号化されたデータ、キーおよびハッシュを受信し、サーバに受信の承認を送信する；
・受信者はキーおよびハッシュを、それとは別に得られたパスワードを使用して解読し、解読されたキーを使用してデータを解読する；
・受信者は解読されたデータのハッシュを計算し、それを受信されたハッシュと比較する。それらが同じならば、別の承認がサーバに送信される；
・受信者が認証された文書を印刷するリクエストをオーソリティに提起した場合、サーバシステムは送信者の定義のデータベース記録をチェックして、彼等が文書の印刷を許可されているかどうか、および彼等が印刷を許可されているコピーの枚数を調べる。満足できる結果が得られた場合、サーバシステムはハッシュにより文書を検証し、プリンタと通信し、印刷のために文書および光学的透かし模様を送信する。印刷の状態を記録するために監査証跡が生成される。
【００５４】［文書認証のための手段］文書の認証のために任意の適切な手段を使用することが可能である。たとえば、特殊なインクおよび特殊な紙は制御された方法で使用されることができる。別の例は、埋込みイメージオブジェクトの多数の層を有する光学的透かし模様を使用することである。光学的透かし模様イメージはサーバシステムに記憶され、サーバシステムによって制御された方法で文書上に印刷するためにプリンタに転送される。サーバシステムによる許可なしに文書が印刷されたならば、その文書上に光学的透かし模様が見出されず、したがってその文書は認証されていないという点で、文書上の光学的透かし模様は認証を行うものである。光学的透かし模様は、その内容がここにおいて参考文献とされている本出願人の別出願の国際特許出願 PCT/SG00/00147 号明細書（“ Optical Watermark”2000年 9月15日シンガポールにおいて出願）に開示されている。
【００５５】光学的透かし模様は、模造および偽造から文書を保護する。それは、多数の目に見えないイメージオブジェクトを反復構造の層の中に埋込み、透かし模様を発生する。その後、たとえば、シール、ロゴまたは背景として透かし模様が文書中に組入れられる。これが“光学的透かし模様”と呼ばれることになる。
【００５６】光学的透かし模様中の模造防止層は、プリ

ンタの性質に敏感である。とくに、それは写真複写機によって検出可能なドットのサイズに依存している。光学的透かし模様の印刷の結果を保証するために、最小の可視ドットサイズおよびその埋込みに対して最良の空間周波数を決定するための較正プロセスが必要である。このプロセスは以下のステップを含んでいる：

・異なるドットサイズを有するテストパターンのアレイを発生し；

・そのプリンタが印刷可能な最小の可視ドットを見出すために、ユーザは印刷されたテストページから第１の可視テストパターンの番号を捜し出し；

・この番号に基づいて、システムは異なった周波数を有するテストパターンのアレイを発生して印刷し；

・情報を最もよく隠蔽することのできる周波数を見出すために、ユーザはこの印刷されたページから第１の可視テストパターンの番号を決定し；

・その２つの番号により、確認ページが印刷され；

・ユーザはその確認ページを写真複写する。コピー防止特徴が認められた場合には、較正は終了する。そうでなければ、成功的な結果が得られるまで、較正が再び行われる。

【００５７】［印刷制御］印刷制御は制御プロセスを行って、文書がオーソリティ／送信者の命令にしたがって厳密に印刷されることを保証する。すなわち、オーソリティ／送信者は、彼等が文書を送信するときに印刷に関する彼等の命令を入力する。その後、この命令はサーバシステムによって実行される。サーバシステムは信頼できる代行業者としてこの命令をデータベース中に文書転送ヒストリの一部分として記憶する。サーバシステムは、送信者によって与えられた命令にしたがって印刷プロセスを制御する。サーバシステムが印刷プロセスを制御するいくつかの方法が存在する。

【００５８】既存の印刷プロセスは制御を全く有しない。クライアントがサーバから文書を受取ったとき、それはスプールシステムによってネットワークに接続されたプリンタに送信されることができる。印刷リクエストがスプールの待ち行列に入るとすぐに、印刷リクエストとクライアント／サーバとの間のリンクは切断される。メッセージは、印刷リクエストが成功したか否かだけである。人々はデータを容易に獲得し、プリンタに対して多数のコピーを印刷するように要求することができる。

【００５９】サーバシステムは信頼できる安全保護されたものなので、クライアントソフトウェアを介してプリンタと通信する。印刷プロセスを確実に制御するために、多くの方法が使用されてもよく、それは受信者を含むことができる。使用される方法はさまざまであり、安全保護されていないプリンタおよび、または秘密保護されていない受信者に対しても異なっている。

【００６０】［安全保護されたプリンタによる印刷制御］安全保護されたプリンタは、クロックと、暗号キー、暗号化および解読用のプログラムおよびデータ用のプログラムを記憶するための安全保護されたメモリと、プログラムの実行、クライアントおよびサーバとの通信、ならびにプリンタの制御を行うためのＣＰＵとを含むハードウェア装置を有している。ハードウェア装置は、それがクロック、キーおよびプログラムならびにランタイムプログラムに対する外部からのアタックを阻止するという点で安全保護されたものである。ユーザが認証されたコピーを印刷することをオーソリティにリクエストしたとき、サーバシステムはプリンタと通信し、クライアントを介したハンドシェークプロセスを完成させる。公開キー対に基づくプリンタおよびサーバシステムの認証が成功した後、サーバシステムは時間スタンプにより暗号化されたハッシュおよび光学的透かし模様と、印刷命令とをプリンタに送信する。セキュリティハンドシェークプロトコルおよび暗号化されたデータ送信に関する詳細については、文献（Chapter 9 “ Security Handshaking Pitfalls, ”p223 in the book of “Network Security-private communication in a public world,” by C. Kaufman,R.Perlman,and M.Speciner,PTR Prentice Hall,1995 ）を参照されたい。

【００６１】プリンタは、その専用キーを安全保護されたメモリ中に記憶する。そのデジタル証明書は、受信者がサービスセンターに登録されたときにサーバシステムに知らされる。セキュリティハンドシェークプロセスを成功的に完成させた後、サーバシステムは暗号化された命令、文書ハッシュおよび光学的透かし模様をプリンタに送信する。全てのデータは時間スタンプおよびデジタル署名により暗号化される。プリンタは、文書をクライアントソフトウェアから受信し、データを解読し、サーバからのデジタル署名および時間スタンプを検証し、その検証が成功した場合にのみそれを印刷する。データは印刷した直後に消去される。プリンタは印刷されたデータのハッシュを生成し、時間スタンプと共にそのハッシュに署名し、監査証跡記録に保持されるようにそれをサーバに送信する。

【００６２】暗号化技術およびＰＫＩに関しては、サーバシステムとプリンタとの間の通信は安全に保護されている。安全に保護されたプリンタは、信頼できる製造業者によって製造され検査されているため、安全保護されたメモリに記憶されたプログラムが不正操作されることは確実に不可能であり、またプリンタのＣＰＵにおいて実行しているプログラムへのランタイムアタックが防止されている。

【００６３】［信頼できるクライアントによる印刷制御］クライアントが信頼できる場合、クライアントソフトウェアに対するアタック、すなわちクライアントソフトウェアプログラムに対するタイムアタックは１つも存在しないはずである。クライアントソフトウェアによって、サーバシステムはプリンタと通信し、その状態をチ

ェックし、印刷命令およびデータを送信し、プロセス全体を監視し、最終的に監査証跡記録を生成する。プリンタとの対話は、たとえば、ヒューレット・パッカード社製のＰＪＬおよびＰＭＬのような利用可能な印刷タスク言語を使用する。図３は、ＰＪＬを使用する印刷制御のフロー図である。印刷制御プロセスにおける基本的なステップは：

・プリンタのＩＰアドレスおよび製造番号をチェックして記録し；

・全てのプリンタタスクに共通するプリンタの設定、特定のプリンタタスクだけに有効な設定を含むプリンタの状態、およびたとえば１５秒毎の、固定したインターバルでのプリンタの状態を読出し；

・現在の印刷タスクに必要とされる全ての設定に対する値を設定し；

・印刷タスクがプリンタに送信されている期間中に別のユーザがその設定に対して不正操作をしないようにするために制御パネルをロックし、制御パネルをロックできない場合、印刷タスクは中止され；

・ＰｏｓｔＳｃｒｉｐｔ（ＰＳ）、印刷制御言語（ＰＣＬ）またはプリンタ用エプソン標準コード（ＥＳＣ／Ｐ）のいずれかを使用して印刷タスクを送信することである。

【００６４】制御プログラムは最初に、プリンタの設定に関する必要な全ての情報を獲得する。この情報により、所望しない構成または設定が所望の設定に再構成される。その後、プリンタはその装置およびページの詳細の報告をたとえば１５秒毎等の予め定められたインターバルで返送するように設定される。これに続いて、印刷タスクがプリンタに送信される。定期的な状態報告により、印刷プロセスは厳密に監視される。本物の用紙ジャムが発生した場合、エラーが報告され、再印刷が行われることができる。印刷が終了した後、プリンタ設定は元の設定に戻すように再構成される。全ての状態報告は監査証跡のために収集される。

【００６５】較正プロセスは、常に人間が介入して行われるわけではない。すなわち、較正は可視ドットサイズ、トナーレベルおよび他のプリンタパラメータを比較するために工場で行なわれる。そのデータにより、プリンタ状態のチェック後に、適切なプリンタ設定が決定され、文書上に印刷される光学的透かし模様の最高性能に対して設定される。

【００６６】［安全保護されていないプリンタを有する安全保護されていないクライアントによる印刷制御］安全保護されていないクライアントまたは信頼できないクライアントは、クライアントソフトウェアおよびハードウェアならびにそのプリンタに対するアタックの可能性を意味する。これらはソフトウェアへのアタック、データを獲得し、サーバに誤情報を与えるためのランタイムアタックを含んでいる。２つの方法があり、１つの方法は可能な限りアタックを免れるクライアントソフトウェアを有することであり、他方の方法はクライアントソフトウェアを保護するための余分なハードウェアを導入することである。クライアントソフトウェアは、分散されたときに基本部分および感応部分という２つの部分に分割される。感応部分は、透かし模様発生機能およびアクセス制御のような感応コードおよびデータを含んでいる。基本部分は、ユーザが登録されたときに分散されインストールされる。

【００６７】クライアントソフトウェアを保護する方法は以下のステップを含んでいてもよい：

・各印刷に対して基本クライアントソフトウェアの正当性を検査すること；クライアントソフトウェアに対する修正は、これを誤動作させる可能性がある。このような修正はネットワークエラー、ユーザのハードディスク中の故障、ウィルス、またはソフトウェアへのアタックのために発生することができる。これを防止するために、基本クライアントソフトウェアが配信される前に、そのソフトウェアのハッシュ結果が計算されてサーバに記憶される。ユーザが印刷をリクエストしたとき、同じハッシュ関数が計算され、その結果が検証のためにサーバに送信される。そのサーバは、ハッシュ結果が前に記憶されたものと同じ場合にのみ印刷データをクライアントに送信する。そうでなければ、印刷は許可されず、ユーザは別のアクションをとるように促される。

【００６８】・リクエスト時に感応コードをダウンロードするか、あるいは感応コードを迅速に解読すること；感応部分は、信頼できるサーバに保持されているか、あるいはクライアントに暗号化されたフォーマットで配信されることができる。それが信頼できるサーバに保持されている場合、それは、基本部分によって安全保護された接続（たとえば、ＳＳＬ）によって要求されたときにクライアントＰＣにダウンロードされ、使用直後に消去される。感応部分はダウンロード時間を短縮するために小さい状態または圧縮された状態に維持される。感応部分はまたクライアントソフトウェアの基本部分と共に、暗号化された形態でクライアントのマシンにインストールされることができる。必要とされた場合には、感応部分はメモリにロードされ、解読されて実行される。サーバが解読キーを管理する。これを行うことによって、コードの分解のような静的アタックは不可能になる。

【００６９】・ハードウェアから感応部分を獲得すること；アタッカーがクライアントソフトウェアをアタックする時間は実質的に無限にあるが、ハードウェアに対するアタックははるかに困難である。したがって、感応部分を印刷中にハードウェアから獲得し、印刷プロセスが終了した直後にメモリから消去することができる。非常に高い技術を有するアタッカーはクライアントソフトウェアにアタックして、無制限に文書のコピーを印刷することに成功することが可能かもしれないが、そのコピー

には認証用の光学的透かし模様がないため、それらは無効であることが一目瞭然である。

【００７０】・ランタイムアタックを検出すること；ランタイムアタック方法の１つは、デバッガーを使用してプログラムをデバッグすることである。いくつかの最新のデバッガーは検出を回避できるため、デバッガーを求めてシステムの中をランタイムでサーチすることは不十分である。ランタイムアタックを検出する効果的な方法は、感応機能に対する実行時間を計算することである。デバッグされている場合、その実行時間は正常なものより著しく遅くなる。これらの感応機能の実行時間を監視するために分離したスレッドが生成される。その時間が要するはずの時間より著しく長いならば、主プロセスは終了される。別のランタイムアタック方法は、システムフックを使用してシステム呼出し活動を監視することである。システム機能呼出しがフックされている間、全ての入出力データはダンプされることができ、これらのデータには解読されたデータまたは機密情報が含まれている可能性がある。この種のアタックを阻止するために、クライアントソフトウェアは全てのシステムフックを列挙し、それらを内部ブラックリストと比較する。ブラックリストに載せられたフックが見出された場合、クライアントソフトウェアは実行を終了する。サーバは上述されたブラックリストを定期的に更新して新しく出現したフックアプリケーションを処理する。

【００７１】［オフライン印刷制御］印刷制御がオフラインの場合、文書の印刷に必要な全ての情報は印刷の前にクライアントのマシンにダウンロードされる。これは以下に示すものを含んでいることが好ましい：

・文書自身；

・送信者の手書きの署名および、または物理的シールのイメージ、および光学的透かし模様を含むシール；このシールは２つの部分：文書の印刷された全てのコピーに共通するシールと、文書の印刷されたコピーのそれぞれに特有の特有のシールにさらに分割される；

・使用制御および監査証跡。

【００７２】この情報は、そのセキュリティを確実にするために特別に設計され暗号化された文書パッケージで配信される。サーバは印刷プロセスに関与しないので、安全保護されたハードウェア／ソフトウェアが、サーバの代わりに動作するクライアントシステム中にインストールされる。したがって、これは２つのソリューション、すなわちハードウェアソリューションとソフトウェアソリューションを提供する。それらは、所望に応じて論理和的に、あるいは論理積的に使用可能である。

【００７３】［ハードウェアソリューション］図４を参照すると、安全保護されたハードウェア装置が、プリンタと統合されていることが好ましいクライアントシステムに結合されている。この装置は以下のものを含んでいることが好ましい：

１．安全保護されたメモリ401 ；これは重要な情報を記憶するために使用される。異なるアクセス権がＣＰＵおよびそのオンチッププログラム403 によって設定される。たとえば、メモリの２つのカテゴリーが存在することができる：

（ａ）ユーザパスワードが入力され検証されたときにアクセス可能なメモリ；

（ｂ）内部使用に対して厳しく制御されているメモリ；たとえば、安全保護されたキーおよび、または製造番号がこのメモリに記憶される。製造番号は特有であることをハードウェア製造業者によって保証されていることが好ましい；

２．ＤＡＲ（読出し後消去）メモリ402 ；このメモリ中のデータは、それが読出された後で自動的に消去される。これはオンチッププログラムまたはハードウェアによって行われてもよい。印刷ライセンスのような重要な情報はこの領域に記憶されている；

３．オンチッププログラム403 を備えたＣＰＵ；これは安全保護されたメモリ401 およびＤＡＲメモリ402 にアクセスし、ユーザリクエスト、暗号化、解読、およびデジタル署名の生成を認証することができる。オンチッププログラムはまた、ファイルシステムであることが好ましいキー管理システムを含んでいる。印刷タスクが到着したとき、タスク識別番号がハードウェアに送信され、その時にキー管理システムが対応したキーを安全保護されたメモリ401 またはＤＡＲメモリ402 から検索する。ＣＰＵはまたタイムアタックを阻止するために安全保護された実時間クロックを含んでいてもよい；

４．インターフェース404 ；これは、ハードウェア装置とホストとの間の通信をセットアップし、盗聴アタックを阻止するためにデータ流を暗号化することができる。

【００７４】安全保護されたメモリおよびＤＡＲメモリの両者に対するハードウェア装置中のメモリ空間は、いくつかのブロックに分割されている。有効なユーザだけが正しいパスワードを与えることによりそれらのブロックにアクセスすることができる。装置はある個数のブロックを含んでいるように設計されており、これらの各ブロックにアクセスするために割当られた最初のパスワードがメモリチップの製造中に割当てられる。特有のユーザＩＤキーは各受信者用の安全保護されたメモリブロック中に記憶され、また、サーバのデータベースに記録される。デジタル証明書を使用したとき、ユーザの専用キーはハードウェア装置400 の安全保護されたメモリブロックに記憶されることができる。

【００７５】ハードウェア装置400 は、そのＣＰＵまたはプリンタのＣＰＵ（利用可能ならば）のいずれかを使用して暗号化／解読動作を行うために十分にパワフルでなければならない。

【００７６】サーバは、信頼できるものであり、ユーザがハードウェアを利用できるようにし、そのハードウェ

ア装置のキーその他のアスペクトを管理することができる。

【００７７】ハードウェア装置はいくつかの方式の１つによって印刷を制御し、以下、これらの方法の２つを例示する：

＜方式１＞この方式は、たとえば、３ＤＥＳ，ＡＥＳ，ＢｌｏｗＦｉｓｈ等の対称的な暗号を使用する。それは図5に示されているように送信者、受信者、印刷装置および信頼できるサーバから構成されている。受信者のハードウェア装置は、ランダムキー（Ｋｅｙ１，…ＫｅｙＮ，ＴＫｅｙ）のいくつかのセットがそれらのブロックのＤＡＲメモリに書込まれている。ＴＫｅｙはトップアップキーを表す。これらのキーはライセンスキーであり、特有のシールを暗号化するために使用される。トップアップキー（ＴＫｅｙ）はトップアッププロセスにおいて使用される。１組の特有ユーザＩＤキーと各キーセットに対応した初期パスワードは、ハードウェア装置の安全保護されたメモリ中に記憶されている。これら全てのキーのコピーもまた信頼できるサーバに記憶されている。送信者および受信者ならびに彼等のハードウェア装置は、安全保護された印刷プロセスを使用する前に、信頼できるサーバに登録されなければならない。

【００７８】［受信者の登録プロセス］受信者は、文書を受信する前に、信頼できるサーバに登録しなければならない。登録プロセスは：

１．受信者はユーザ名、ｅメールアドレスのような彼等の情報および彼等のハードウェア装置のＩＤを提供することによってサーバにおける登録をリクエストする；

２．サーバは受信者のリクエストを処理する。認可された場合、サーバはそのハードウェア装置の使用されていないユーザＩＤを求めてそのデータベースをサーチする。全てのユーザＩＤが使用されている場合、新しいハードウェア装置がインストールされなければならない；

３．サーバはユーザの情報を記録し、初期パスワードおよびユーザＩＤインデックスを受信者に送信する；

４．クライアントソフトウェアがまだインストールされていない場合には、受信者のマシンにインストールされる；

５．受信者は彼等のユーザ名、初期パスワードおよびユーザＩＤインデックスを入力することによりクライアントソフトウェアにログオンする；

６．ユーザＩＤインデックスおよび初期パスワードはハードウェア装置に送信され、それの対応した、そのユーザに対するブロックを活動化する；

７．受信者は、彼等のパスワードを直ぐに変更するように促され、初期パスワードはその新しいパスワードによって置換される；

８．クライアントソフトウェアは、そのユーザに対する私設ディレクトリを準備し、そのディレクトリのキー（ディレクトリキーと呼ばれる）をハードウェア装置中のそのユーザのメモリブロックに記憶する。

【００７９】［ライセンスキートップアッププロセス］図６乃至８に示されているように、ユーザが装置中に記憶されている彼等のライセンスキーを使用した場合、あるいは新しいリクエストに対してライセンスが不十分である場合、ユーザは以下のプロセスを使用して彼等のライセンスキーをトップアップする必要がある：

１．文書に対するＭ個のライセンスキーを受信者に送信する送信者のリクエストをサーバが受信し、その受信者のライセンスキーがそのタスクにとって不十分であるとサーバが認めた場合、サーバはトップアッププロセスを開始する；あるいは、

２．たとえば、その受信者が十分なキーを有しない、受信者のキーが全て使用されている、もしくは受信者がもっと多くのコピーを印刷することを希望している等の理由のために、受信者は彼等のライセンスキーのトップアップに対するリクエストを行う；

３．サーバはそのリクエストを処理する。認可された場合、サーバは１つの新しいキーセットＫｅｙ１´乃至ＫｅｙＸ´および新しいトップアップキー（ＴＫｅｙ´）を発生する；

４．この新しいキーセットは受信者のＴｋｅｙ´により暗号化される；

５．この新しいキーセットに対するハッシュが計算され、トップアップキーセットを形成するために受信者のＩＤキーを使用してその新しいキーセットと共に暗号化される；

６．トップアップキーセットは文書パッケージと共に、あるいは別々に受信者に送信される；

７．受信者は、データを検索した後、トップアップキーセットを彼等のハードウェア装置に送信する；

８．この装置は受信者のＩＤキーによりデータを解読し、完全性チェックを行うためにそのデータのハッシュを計算する；

９．そのデータにエラーがある場合、装置はＴＫｅｙ´をＤＡＲメモリから読出して、そのキーセットを解読する；

１０．その後、この装置はＤＡＲメモリ中のキーセットを更新する。新しいキーセットは、そのインデックス番号が前の最後のキーから連続しているため、使用されていないキーに重書きしない；

１１．ＤＡＲメモリ中の前のトップアップキー（Ｔｋｅｙ）は新しいトップアップキーＴｋｅｙ´によって置換される。

【００８０】送信者が文書を受信者に送信するために：

１．送信者は彼等のユーザＩＤおよびパスワードを使用して安全保護されたリンク（たとえばＳＳＬ）によって信頼できるサーバに接続する；

２．認証に成功した後、送信者は彼等の文書を以下のステップによって処理する：

（ａ）文書またはそのハッシュ結果、共通シール、送信に対する時間スタンプ、および文書の満期日をセッションキー１により暗号化する；
（ｂ）その文書の本文、満期日、およびステップ（ａ）の結果に対してハッシュ結果が計算される。その後、これらの３つの部分がセッションキー２で暗号化され；
（ｃ）その後ステップ（ｂ）の結果と、受信者のＩＤと、セッションキー１と、暗号化するために使用されたセッションキー２と、その受信者が文書のM個のコピーを印刷するためのライセンスの数（たとえば、Ｍ）と、およびM個の特有のシールとをサーバに送信し、Mは見るだけを示すゼロであってもよい；
３．サーバは受信者の情報の正当性を検査し、その後M個のライセンスキー（Ｋｅｙ１乃至ＫｅｙＭ）をランダムに、または順番に受信者のキーセットから選択する；
４．M個の特有のシールおよびセッションキー１がＫｅｙ１およびＫｅｙＭにより別々に暗号化されてM個のライセンスを形成する。ライセンスパック全体のハッシュフィールドが計算され、そのライセンスに対する完全性チェックが行われる；
５．その後、サーバは、送信者が準備した文書本文［上記のステップ２の（ｂ）の結果］と、受信者のＩＤキーにより暗号化されたセッションキー２と、およびライセンスとを含む文書パッケージ（図６）を生成する。受信者が文書を印刷することを送信者が許可していない場合、ライセンスフィールドは空である。受信者が有しているライセンスキーが不十分である場合にもトップアップキーセットが準備される；
６．サーバは通知を受信者に送信し、その文書パッケージがいつでも収集できることを彼等に知らせる。
【００８１】受信者は、上記の（６）において通知を受取る前または後の任意の時点でサーバに接続することができる。その後、受信者は彼等に対するデータが存在しているかどうかをチェックすることができる。受信者が文書を見て印刷するための手順は次のとおりである：
１．受信者は彼等のユーザ名およびパスワードを使用して安全保護されたリンク（たとえば、ＳＳＬ）によって信頼できるサーバに接続する；
２．サーバはチャレンジ応答シーケンスを供給することによりそのユーザの正当性を検査し、このチャレンジ応答シーケンスは：
（ａ）サーバがユーザ名の正当性を検査し、その後データベースからユーザのＩＤキーを検索する；
（ｂ）サーバが乱数を選択または発生し、受信者のＩＤキーを使用してそれを暗号化し、それを受信者に返送する；
（ｃ）受信者のＩＤキーにアクセスするために彼等のパスワードがハードウェア装置に送信される；
（ｄ）ハードウェア装置がＩＤキーを使用して、暗号化された乱数を解読する；
（ｅ）乱数がサーバに返送される；
（ｆ）サーバは乱数を検証することによってユーザを認証する；
３．認証の成功後、クライアントソフトウェアはその受信者に対するデータをサーバからダウンロードする；
４．データを受信した後、受信者はサーバとの接続を切断するか、あるいはオンライン状態のままでいることができる；
５．クライアントソフトウェアは、トップアップキーセットが存在しているか否かをチェックし、存在するならば、ライセンスキーのトップアップのために、最初にトップアップキーセットがその装置に送信される；
６．クライアントソフトウェアは解読のために、暗号化されたセッションキー２を装置に送信する。セッションキー２は解読され、クライアントソフトウェアに戻され、その後このクライアントソフトウェアが文書パッケージを解読し、文書パッケージ中のハッシュフィールドをチェックする。ハッシュチェックに不合格の場合、受信者はサーバにリソリューションを提供するように告げる。暗号化された文書またはそのハッシュ、共通シール、時間スタンプ、および満期日はこの時点では解読されていない；
７．その後、文書パッケージは再度暗号化され、ディレクトリキーを使用して受信者の私設ディレクトリに記憶される。
【００８２】受信者が文書を見たいと望んだ場合、以下の手順が行われる：
１．受信者が彼等のユーザ名とパスワードによりクライアントソフトウェアにログオンし、ハードウェア装置によって認証される；
２．認証が成功した後、クライアントソフトウェアが受信者のディレクトリキーを読出し、文書パッケージに対する受信者の私設ディレクトリにアクセスする；
３．満期日がハードウェア装置中の内部クロックと比較される。満期日が過ぎていることを内部クロックが示した場合には、その文書は期限切れであり、それを見ることは許されない；
４．文書が期限切れでない場合、受信者はその文書を見ることができる。
【００８３】受信者が文書の印刷を希望した場合、以下の手順が行われる：
１．受信者が彼等のユーザ名とパスワードによりクライアントソフトウェアにログオンし、ハードウェア装置によって認証される；
２．認証が成功した後、クライアントソフトウェアが受信者のディレクトリキーをハードウェア装置から読出し、文書パッケージに対する受信者の私設ディレクトリにアクセスする；
３．解読のために、クライアントソフトウェアは使用されていないライセンスをハードウェア装置に送信する；

４．ハードウェア装置は、インデックスにしたがって受信者のＤＡＲメモリからキーを読出し、セッションキー１および特有のシールを解読する；
５．解読のために、文書またはそのハッシュ、共通シール、時間スタンプ、および満期日が装置に送信される。満期日がその装置内のクロックと比較される。満期日が過ぎていることを内部クロックが示した場合には、その文書は期限が切れており、印刷は許可されない。装置内でハードウェア故障が生じている場合、ユーザはハードウェア供給元にその問題を解決するように告げなければならない；
６．クライアントソフトウェアは、上記のステップ５から得られる解読された文書ハッシュを使用して文書の完全性を検証し、その文書をプリンタに送信するか、あるいは解読された文書をプリンタに送信する；
７．クライアントソフトウェアはプリンタと通信し、印刷状態を監視し、文書が適当なシールを付けられて印刷される；
８．監査証跡情報が発生され、各コピーが印刷された後にハードウェア装置内のプログラムによって受信者のＩＤキーで署名され、それによって印刷された各コピーが拒否されることのできないものになる；
９．監査証跡情報がハードウェア中に記憶され、サーバに周期的にアップロードされる。サーバはこの監査証跡を予め定められた期間のあいだ維持する。予め定められた期間の終了後、それはサーバから削除される。
【００８４】＜方式２＞図９を参照すると、ハードウェア装置中のＤＡＲメモリは、それが製造されたときは空のままにされている（すなわち、ゼロを書込まれている）。必要な全てのキーのコピーもまた信頼できるサーバに記憶されている。全ての送信者および受信者、ならびに彼等のハードウェア装置は、それらが安全保護された印刷プロセスを使用することができる前に、信頼できるサーバにまとめて登録されていなければならない。
【００８５】受信者の登録プロセスは、方式１において述べたものと同じであり、以下のステップを含んでいる：
１．送信者は、彼等のユーザＩＤおよびパスワードを使用して安全保護されたリンク（たとえば、ＳＳＬ）によって信頼できるサーバに接続し；
２．認証に成功した後、送信者は彼等の文書を以下のステップによって処理する：
（ａ）文書またはそのハッシュ、共通シール、送信に対する時間スタンプ、および文書の満期日をセッションキー１によって暗号化する；
（ｂ）その文書本文、満期日、およびステップ（ａ）の結果に対してハッシュ結果が計算される。その後、これらの３つの部分がセッションキー２によって暗号化され；
（ｃ）ステップ（ｂ）の結果、受信者のＩＤ、セッションキー１、暗号化するために使用されたセッションキー２、その受信者が文書のM個のコピーを印刷するためのライセンスの数（たとえば、Ｍ）、およびＭ個の特有のシールをサーバに送信し、この場合Mが見るだけを示すゼロであってもよい；
３．サーバが受信者の情報の正当性を検査し、図１１に示されているようにライセンスおよびライセンスインストーラを生成する；
４．ライセンスはセッションキー１と、Ｍ個のサーバ発生ランダムライセンスキーＫｅｙ１乃至ＫｅｙＭにより暗号化されたＭ個の特有のシールとを含んでいる；
５．ライセンスインストーラは、その文書に対する特有ＩＤを含んでいる。それはまた時間スタンプ（ライセンスインストーラが生成された時間）と、満期日とを含んでいる。このライセンスインストーラは受信者のＩＤキーにより暗号化される；
６．完全性チェックのために、ライセンスおよびライセンスインストーラのハッシュもまた計算される；
７．その後、サーバは図１０に示されている文書パッケージを生成し、これは送信者の処理した文書パッケージ［ステップ２の（ｂ）の結果］と、受信者のＩＤキーにより暗号化されたセッションキー２と、ライセンスと、およびライセンスインストーラとを含んでいる。受信者が文書を印刷することを送信者が許可するつもりがない場合、ライセンスおよびライセンスインストーラに対するフィールドは空である；
８．サーバは、その文書が収集に利用可能であることの通知を受信者に送信する。
【００８６】受信者はこのような通知を受取って、あるいは受取らずに、サーバに接続し、彼等に対する文書および、またはデータが存在しているかどうかをチェックすることができる。受信者が文書を見て印刷するための手順は次のとおりである：
１．受信者は彼等の受信者名およびパスワードを使用して安全保護されたリンク（たとえば、ＳＳＬ）によって信頼できるサーバに接続する；
２．サーバはチャレンジ応答シーケンスを生成することによりその受信者の正当性を検査し、このチャレンジ応答シーケンスは：
（ａ）サーバが受信者の名前の正当性を検査し、その後データベースからその受信者のＩＤキーを検索する；
（ｂ）サーバは乱数を発生し、受信者のＩＤキーを使用してそれを暗号化し、それを受信者に返送する；
（ｃ）受信者のＩＤキーにアクセスするために受信者のパスワードが受信者のハードウェア装置に送信される；
（ｄ）受信者のハードウェア装置はＩＤキーを使用して、暗号化された乱数を解読する；
（ｅ）乱数がサーバに返送される；
（ｆ）サーバは乱数を検証することによって受信者を認証する；

３．認証の成功後、その受信者は彼等に対する文書および、またはデータをサーバからダウンロードする；
４．文書および、またはデータを受信した後、受信者はサーバとの接続を切断するか、あるいはオンライン状態のままでいることができる；
５．クライアントソフトウェアは、インストールのために受信者のハードウェア装置にライセンスインストーラを送信する；
６．そのハードウェア装置は受信者のＩＤキーを使用してライセンスインストーラを解読し、ハッシュフィールドを検証することによってライセンスインストーラの完全性をチェックする。検証が失敗した場合、受信者はその問題を解決するためにサーバに知らせる；
７．装置はＩＤの保管されたリストにより文書ＩＤをチェックする；
８．ＩＤが見つからない場合、その装置内のクロックに対して時間スタンプおよび満期日がチェックされる；
９．全てのチェック手順が成功的に終了することにより、ライセンスキーが受信者のＤＡＲメモリにインストールされ、ＩＤが安全保護されたメモリ中のＩＤリスト中に記憶される；
１０．解読のために、クライアントソフトウェアは暗号化されたセッションキーをハードウェア装置に送信する。このハードウェア装置はセッションキー２を解読し、それをクライアントソフトウェアに返送し、その後このクライアントソフトウェアが文書パッケージを解読し、文書パッケージ中のハッシュフィールドをチェックする。チェックが失敗した場合、受信者はサーバに通知してリソリューションを提供するように要求する。暗号化された文書またはそのハッシュ、共通シール、時間スタンプ、および満期日はこの時点では解読されていない；
１１．その後、文書パッケージは再度暗号化され、ディレクトリキーを使用して受信者の私設ディレクトリに記憶される。
【００８７】文書を見るための手順は次のとおりである：
１．受信者が彼等のユーザ名とパスワードによりクライアントソフトウェアにログオンし、ハードウェア装置によって認証される；
２．認証が成功した後、クライアントソフトウェアが受信者のディレクトリキーを読出し、文書パッケージに対する受信者の私設ディレクトリにアクセスする；
３．満期日がハードウェア装置内のクロックと比較される。満期日が過ぎていることを内部クロックが示した場合には、その文書は期限切れであり、それを見ることは許されない；
４．文書が期限切れ出ない場合、受信者はそれを見ることができる。
【００８８】文書を印刷する手順は次のとおりである：
１．受信者が彼等のユーザ名とパスワードによりクライアントソフトウェアにログオンし、ハードウェア装置によって認証される；
２．認証が成功した後、クライアントソフトウェアが受信者のディレクトリキーを読出し、文書パッケージに対する受信者の私設ディレクトリにアクセスする；
３．解読のために、クライアントソフトウェアは使用されていないライセンスをハードウェア装置に送信する；
４．ハードウェア装置は、インデックスにしたがって受信者のＤＡＲメモリからキーを読出し、セッションキー１および特有のシールを解読する；
５．解読のために、文書またはそのハッシュ、共通シール、時間スタンプ、および満期日が装置に送信される。満期日がその装置内のクロックと比較される。満期日が過ぎていることを内部クロックが示した場合には、その文書は期限切れであり、印刷は許可されない。装置内でハードウェア故障が生じている場合、ユーザはその問題をハードウェア供給元に通知し、その問題を解決することを彼等に要求しなければならない；
６．クライアントソフトウェアは、上記のステップ５の解読された文書ハッシュを使用して文書の完全性を検証し、その文書をプリンタに送信するか、あるいは解読された文書をプリンタに送信する；
７．クライアントソフトウェアはプリンタと通信し、印刷プロセスの状態を監視し、文書が適当なシールを付けられて印刷される；
８．監査証跡情報が発生され、各コピーが印刷された後にハードウェア装置内のプログラムによって受信者のＩＤキーを使用して署名され、それによって印刷された各コピーが拒否されることのできないものになる；
９．ハードウェア装置はＩＤリストを周期的にチェックして、期限切れのＩＤを消去する；
１０．監査証跡情報はハードウェア装置に記憶され、サーバに周期的にアップロードされる。サーバはこの監査証跡を予め定められた期間のあいだ維持する。それは予め定められた期間の終了時に消去される。
【００８９】ハードウェア装置内のＣＰＵが暗号化／解読動作の全てを行うほど十分なパワフルさを有しない場合、あるいはインターフェースの速度が印刷要求を満たには不十分である場合、ハードウェア装置は、図１２に示されているように、印刷プロセスにおいて安全保護された記憶トークンとして使用される。ハードウェア装置は以下のものを含んでいる：
１．安全保護されたメモリ1201；これは重要な情報を記憶するために使用される。このメモリは、ユーサパスワードが入力され検証された場合にアクセス可能である。その製造番号はハードウェア製造業者によって特有のものであることが保証されていることが好ましい；
２．インターフェース1202；これは、装置とホスト間の通信を設定すると共に、盗聴アタックを阻止するために

データ流を暗号化することができる；
３．バックアップ電池を備えた随意のハードウェアクロック1203；これは、ある時間感応動作が必要になったときに時間基準を提供する。
【００９０】ハードウェア装置は前の方式ほどパワフルではないため、ライセンスキーのインストールおよび管理プロセスはクライアント側のソフトウェアによって行われてもよく、またインターフェースの盗聴防止機能によって保護されてもよい。
【００９１】ハードウェア装置は、マシンのＵＳＢポート、シリアルポートまたはパラレルポートを介してクライアントマシンに結合されることができる。スマートカード、ＵＳＢキーまたはパラレルポートドングル等のいくつかの既製の安全保護された装置がハードウェア装置として使用されることができる。各ユーザは彼等自身のハードウェア装置を有しており、それは、必要とされたときにユーザのマシンに結合され、使用後に取外されることができる。
【００９２】サーバは、信頼できる場所に配置される。それは、送信者中心モデルのような送信者側の場所であることができる。その代りに、それは独立した信頼できるパーティの場所であることができる。サーバのマネージャは、ユーザへのハードウェア装置の供給およびハードウェア装置用のキーの管理を行うことができる。
【００９３】ハードウェア装置は、以下の方式によって印刷を制御する：
＜方式１＞この方式は、たとえば３ＤＥＳ、ＡＥＳ、ＢｌｏｗＦｉｓｈ等の対称的な暗号を使用する。図１３に示されているように、それは送信者、受信者、印刷装置、および信頼できるサーバを含んでいてもよい。
【００９４】受信者のハードウェア装置は、その安全保護されたメモリ中に１組のランダムキー（Ｋｅｙ１、…ＫｅｙＮ、ＴＫｅｙ）を有している。ランダムキーは、ライセンスキーであり、特有のシールを暗号化するために使用される。ＴＫｅｙ（トップアップキー）はトップアッププロセスにおいて使用される。信頼できるサーバ中にはこれら全てのキーのコピーもまた記憶されている。安全保護された印刷プロセスを使用する前に、全ての送信者および受信者、ならびに彼等のハードウェア装置が信頼できるサーバに登録されていなければならない。
【００９５】受信者の登録プロセスは、上述されたものよりいくぶん容易であり、以下のステップを含んでいる：
１．受信者は、たとえばユーザ名、ｅメールアドレスのような彼等の情報を与えることによってサーバに登録することをリクエストする；
２．サーバシステムはその受信者用にハードウェア装置をカストマイズし、このハードウェア装置はその安全保護されたメモリ中に特有ＩＤキー、一連のライセンスキーおよびトップアップキーを有している。その後、これらのキーのコピーがサーバのデータベースに記録される。初期パスワードもまたその装置に割当られる；
３．この装置およびその初期パスワードは受信者に別々に送信され、クライアントソフトウェアが受信者のマシンに前にインストールされていない場合にはインストールされる；
４．受信者は彼等のユーザ名および初期パスワードを入力することによってクライアントソフトウェアにログオンする；
５．初期パスワードは検証のためにハードウェア装置に送信される。そのパスワードが正しければ、受信者は彼等のパスワードを変更するように促される；
６．初期パスワードは、新しいパスワードと置換される；
７．クライアントソフトウェアはそのユーザの専用ディレクトリを準備し、そのディレクトリのキー（ディレクトリキーと呼ばれる）をそのハードウェア装置の安全保護されたメモリに記憶する。
【００９６】［ライセンスキートップアッププロセス］装置のランダムキーが全て使用されているか、あるいは新しいタスクには不十分である場合、その装置はそのランダムキーをトップアップすることが必要になる：
１．サーバが送信者のリクエストを受信して文書に対するＭ個のライセンスキーを受信者に送信したとき、サーバは受信者のライセンスキーをチェックし、必要ならば、トップアッププロセスを開始する；あるいは、
２．たとえば、受信者が十分なキーを有しないか、受信者のキーが全て使用されているか、あるいは受信者がもっと多くのコピーの印刷を必要としている場合、受信者がそのライセンスキーのトップアップをリクエストし；その後、
３．サーバがそのリクエストを処理する。認可された場合、サーバは新しい１組のキーＫｅｙ１´乃至ＫｅｙＸ´および新しいトップアップキーＴＫｅｙ´を発生する；
４．新しい１組のキーは受信者のＴＫｅｙにより暗号化される；
５．新しいキーセットに対するハッシュが計算され、トップアップキーセットを形成するために受信者のＩＤキーを使用して暗号化された新しいキーセットと共に暗号化される；
６．トップアップキーセットは文書パッケージと共に、あるいは別々に受信者に送信される；
７．受信者が文書パッケージを検索した後、受信者はトップアップキーセットをハードウェア装置に送信する；
８．ハードウェア装置はそのＩＤキーにより文書パッケージを解読し、完全性チェックのためにそのデータのハッシュを計算する；
９．エラーがない場合、ハードウェア装置はその安全保

護されたメモリからＴｋｅｙを読出してキーセットを解読する；
１０．その後、ハードウェア装置は安全保護されたメモリ中のキーセットを更新する。新しいキーセットは、そのインデックス番号が前の最後のキーから連続しているので、使用されていないキーに重書きしない；
１１．安全保護されたメモリ中のトップアップキー（ＴＫｅｙ）が新しいトップアップキー（ＴＫｅｙ´）と置換される。
【００９７】送信者が受信者に文書を送信するために：
１．送信者は彼等のユーザＩＤおよびパスワードを使用して安全保護されたリンク（たとえばＳＳＬ）によって信頼できるサーバに接続される；
２．認証に成功した後、送信者は彼等の文書を以下のステップによって処理する：
（ａ）文書またはそのハッシュ、共通シール、送信に対する時間スタンプ、および文書の満期日をセッションキー１により暗号化する；
（ｂ）その文書本文、満期日、およびステップ（ａ）の結果に対してハッシュ結果が計算される。その後、これらの３つの部分の全てがセッションキー２により暗号化され；
（ｃ）その後ステップ（ｂ）の結果と、受信者のＩＤと、セッションキー１と、暗号化するために使用されたセッションキー２と、その受信者が文書のM個のコピーを印刷するためのライセンスの数（たとえば、Ｍ）と、およびM個の特有のシールとをサーバに送信し、Mは見るだけを示すゼロであってもよい；
３．サーバが受信者の情報の正当性を検査し、その後M個のライセンスキーＫｅｙ１乃至ＫｅｙＭをランダムに、または順番に受信者のキーセットから選択する；
４．M個の特有のシールおよびセッションキー１はＫｅｙ１およびＫｅｙＭにより別々に暗号化されてM個のライセンスを形成する。各ハッシュフィールドが計算され、そのライセンスに対する完全性チェックが行われる；
５．その後、サーバは、送信者が処理した文書パッケージ［ステップ２の（ｂ）の結果］と、受信者のＩＤキーによって暗号化されたセッションキー２と、およびライセンスとを含む図１４に示されている文書パッケージを生成する。受信者が文書を印刷することを送信者が許可していない場合、ライセンスおよびトップアップキー用のフィールドは空である。受信者が有しているライセンスキーが不十分である場合、トップアップキーセットが準備される；
６．サーバは、その文書がいつでも収集できるという通知を受信者に送信する。
【００９８】受信者は通知を受取る前またはその後でサーバに接続して、彼等に対するデータが存在しているかどうかをチェックすることができる。受信者が文書を見て印刷するための手順は次のとおりである：
１．受信者は彼等のユーザ名およびパスワードを使用して安全保護されたリンク（たとえば、ＳＳＬ）によって信頼できるサーバに接続される；
２．サーバはチャレンジ応答シーケンスを生成することによりそのユーザの正当性を検査し、このチャレンジ応答シーケンスは：
（ａ）サーバはユーザ名の正当性を検査し、その後データベースからユーザのＩＤキーを検索する；
（ｂ）サーバは乱数を再度発生し、受信者のＩＤキーを使用してそれを暗号化し、それを受信者に送信する；
（ｃ）受信者のＩＤキーにアクセスするために彼等のパスワードがハードウェア装置に送信される；
（ｄ）ハードウェア装置はＩＤキーを使用して、暗号化された乱数を解読する；
（ｅ）乱数がサーバに返送される；
（ｆ）サーバは乱数を検証することによってユーザを認証する；
３．認証の成功後、クライアントソフトウェアはその受信者に対するデータをサーバからダウンロードする；
４．データを受信した後、受信者はサーバとの接続を切断するか、あるいはオンライン状態のままでいることができる；
５．クライアントソフトウェアは、トップアップキーセットが存在しているか否かをチェックし、存在するならば、トップアップのために、最初にトップアップキーセットがその装置に送信される；
６．クライアントソフトウェアは解読のために、暗号化されたセッションキー２をハードウェア装置に送信する。解読されてハードウェア装置から戻されたセッションキー２により、このクライアントソフトウェアが文書パッケージを解読し、その文書パッケージ中のハッシュフィールドをチェックする。このチェックが失敗した場合、受信者は、サーバが問題を解決するようにこの問題をそのサーバに通知する。暗号化された文書またはそのハッシュ、共通シール、時間スタンプ、および満期日はこの時点では解読されていない。
【００９９】その後、文書パッケージはディレクトリキーを使用して受信者の専用ディレクトリに記憶される。
【０１００】受信者が文書を見るために、以下の手順が必要である：
１．受信者が彼等のユーザ名とパスワードによりクライアントソフトウェアにログオンし、ハードウェア装置によって認証される；
２．認証が成功した後、クライアントソフトウェアが受信者のディレクトリキーをその装置から読出し、文書パッケージに対する受信者の専用ディレクトリにアクセスする；
３．満期日および時間スタンプがハードウェア装置内のクロックと比較される。満期日が過ぎていることを内部

クロックが示した場合には、その文書は期限切れであり、それを見ることは許されない；
４．文書が期限切れでない場合、受信者はそれを見ることができる。
【０１０１】受信者が文書を印刷するために、以下の手順が必要である：
１．受信者が彼等のユーザ名とパスワードによりクライアントソフトウェアにログオンし、ハードウェア装置によって認証される；
２．認証が成功した後、クライアントソフトウェアが受信者のディレクトリキーをハードウェア装置から読出し、文書パッケージに対する受信者の専用ディレクトリにアクセスする；
３．クライアントソフトウェアは印刷するライセンスを選択する。入手できるライセンスがない場合、印刷は許可されない；
４．ハードウェア装置は安全保護されたメモリ中からライセンスキーを読出し、セッションキー１および特有のシールを解読し、使用されたライセンスキーを消去する；
５．文書またはそのハッシュ、共通シール、時間スタンプ、および満期日がセッションキー１を使用して解読される。満期日がその装置内のクロックと比較される。満期日が過ぎていることを内部クロックが示した場合には、その文書は期限が切れており、印刷は許可されない。装置内でハードウェア故障が生じている場合、ユーザはハードウェア供給元に通知し、彼等にその問題を解決するように要求する；
６．クライアントソフトウェアは、上記のステップ５の解読された文書ハッシュを使用して文書の完全性を検証し、その文書をプリンタに送信するか、あるいは解読された文書をプリンタに送信する；
７．クライアントソフトウェアはプリンタと通信し、印刷状態を監視し、文書が適当なシールを付けられて印刷される；
８．監査証跡情報が発生され、各コピーが印刷された後に受信者のＩＤキーで署名され、それによって印刷された各コピーが拒否されることのできないものになる；
９．監査証跡情報がハードウェア装置に記憶され、サーバに周期的にアップロードされる。サーバはこの監査証跡を予め定められた期間中維持する。予め定められた期間の終了後、監査証跡情報は消去される。
【０１０２】＜方式２＞図１７に示されているようなこの方式において、ハードウェア装置中の安全保護されたメモリは、それが製造されたときは空である（ゼロを書込まれている）。全ての送信者および受信者、ならびに彼等のハードウェア装置は、本発明の安全保護された印刷プロセスを使用する前に、信頼できるサーバに登録されていなければならない。
【０１０３】受信者の登録プロセスは、上述されたものより若干容易である：
１．送信者は、ユーザ名およびｅメールアドレスのような彼等の情報を提供することによりサーバへの登録をリクエストする；
２．サーバシステムはその受信者用にハードウェア装置をカストマイズし、このハードウェア装置はその安全保護されたメモリに書込まれた特有のＩＤキーを有している。その後、このＩＤキーのコピーがサーバのデータベースに記録される。初期パスワードもまたそのハードウェア装置に割当られる；
３．このハードウェア装置およびその初期パスワードは受信者に別々に送信され、クライアントソフトウェアが受信者のマシンにインストールされる；
４．受信者は彼等のユーザ名および初期パスワードを入力することによってクライアントソフトウェアにログオンする；
５．初期パスワードは検証のためにハードウェア装置に送信される。そのパスワードが正しければ、受信者は彼等のパスワードを変更するようにプロンプトされる；
６．初期パスワードは、新しいパスワードと置換される；
７．クライアントソフトウェアはそのユーザの専用ディレクトリを準備し、そのディレクトリに対するキー（ディレクトリキーと呼ばれる）をそのハードウェア装置の安全保護されたメモリに記憶する。
【０１０４】ユーザが文書を送信するために行う手順は次のとおりである：
１．送信者は彼等のユーザＩＤおよびパスワードを使用して安全保護されたリンク（たとえばＳＳＬ）によって信頼できるサーバに接続する；
２．認証に成功した後、送信者は彼等の文書を以下のステップによって処理する：
（ａ）文書またはそのハッシュ、共通シール、送信に対する時間スタンプ、および文書の満期日をセッションキー１により暗号化する；
（ｂ）その文書本文、満期日、およびステップ（ａ）の結果に対してハッシュ結果が計算される。その後、３つの部分の全てがセッションキー２により暗号化される；
（ｃ）ステップ（ｂ）の結果と、受信者のＩＤと、セッションキー１と、暗号化するために使用されたセッションキー２と、その受信者が文書のＭ個のコピーを印刷するためのライセンスの数（たとえば、Ｍ）と、およびＭ個の特有のシールとをサーバに送信し、Ｍは見るだけを示すゼロであってもよい；
３．サーバが受信者の情報の正当性を検査し、図１９に示されているようにライセンスおよびライセンスインストーラを生成する；
４．ライセンスはセッションキー１と、Ｍ個のサーバ発生ランダムライセンスキーＫｅｙ１乃至ＫｅｙＭにより暗号化されたＭ個の特有のシールとを含んでいる；

５．ライセンスインストーラは、その文書に対する特有ＩＤを含んでいる。それはまた時間スタンプ（ライセンスインストーラが生成された時間）と、満期日とを含んでいる。このライセンスインストーラは受信者のＩＤキーにより暗号化される；
６．完全性チェックのために、ライセンスおよびライセンスインストーラのハッシュもまた計算される；
７．その後、サーバは図１８に示されている文書パッケージを生成し、これは送信者の処理した文書パッケージ［ステップ２の（ｂ）の結果］と、受信者のＩＤキーにより暗号化されたセッションキー２と、ライセンスと、およびライセンスインストーラとを含んでいる。送信者が受信者による文書の印刷を意図しない場合、ライセンスおよびライセンスインストーラフィールドは空である；
８．サーバは、その文書が収集する準備ができたという通知を受信者に送信する。
【０１０５】受信者は、このような通知を受取る前またはその後でサーバに接続し、彼等に対する文書が存在しているかどうかをチェックできる。受信者が文書を見て印刷するための手順は：
１．受信者が彼等のユーザ名およびパスワードを使用して安全保護されたリンク（たとえば、ＳＳＬ）によって信頼できるサーバに接続される；
２．サーバがチャレンジ応答シーケンスを生成することによりそのユーザの正当性を検査し、このチャレンジ応答シーケンスは：
（ａ）サーバはユーザ名の正当性を検査し、その後データベースからユーザのＩＤキーを検索する；
（ｂ）サーバは乱数を発生し、受信者のＩＤキーを使用してそれを暗号化し、それを受信者に返送する；
（ｃ）受信者のＩＤキーにアクセスするために彼等のパスワードがハードウェア装置に送信される；
（ｄ）ハードウェア装置はＩＤキーを使用して、暗号化された乱数を解読する；
（ｅ）乱数がサーバに返送される；
（ｆ）サーバは乱数を検証することによってユーザを認証する；
３．認証の成功後、受信者は彼等に対するデータをサーバからダウンロードする；
４．データを受信した後、受信者はサーバとの接続を切断するか、あるいはオンライン状態のままでいることができる；
５．クライアントソフトウェアはインストールのためにハードウェア装置にライセンスインストーラを送る；
６．ハードウェア装置は受信者のＩＤキーを使用してライセンスインストーラを解読し、ライセンスインストーラのハッシュフィールドを検証することによりその完全性をチェックする。チェックが失敗であった場合、受信者はサーバに通知し、その問題を解決するようにサーバに要求する；
７．ハードウェア装置はそれに保管されているＩＤのリストにより文書ＩＤをチェックする。ＩＤが見出されなかった場合、時間スタンプおよび満期日がその装置内のクロックに対してチェックされる。
【０１０６】８．全てのチェックが成功してしまうと、ライセンスキーが安全保護されたメモリにインストールされ、ＩＤが安全保護されたメモリ中のＩＤリストに記憶される；
９．クライアントソフトウェアは解読のために、暗号化されたセッションキー２をハードウェア装置に送信する。ハードウェア装置はセッションキー２を解読し、それをクライアントソフトウェアに戻し、その後このクライアントソフトウェアが文書パッケージを解読し、文書パッケージ中のハッシュフィールドをチェックする。チェックが失敗であった場合、受信者はサーバに通知し、問題を解決するようにサーバに要求する。暗号化された文書またはそのハッシュ、共通のシール、時間スタンプ、および満期日はこの時点では解読されていない；
１０．その後、文書パッケージは再度暗号化され、ディレクトリキーを使用して受信者の専用ディレクトリに記憶される。
【０１０７】受信者が文書を見るための手順は：
１．受信者が彼等のユーザ名とパスワードによりクライアントソフトウェアにログオンし、ハードウェア装置によって認証される；
２．認証が成功した後、クライアントソフトウェアが受信者のディレクトリキーを読出し、文書パッケージに対する受信者の専用ディレクトリにアクセスする；
３．満期日がハードウェア装置中のクロックと比較される。満期日が過ぎていることを内部クロックが示した場合には、その文書は期限切れであり、それを見ることは許されない；
４．文書の期限が切れていない場合、受信者はそれを見ることができる。
【０１０８】受信者が文書を印刷するための手順は：
１．受信者が彼等のユーザ名とパスワードによりクライアントソフトウェアにログオンし、ハードウェア装置によって認証される；
２．認証が成功した後、クライアントソフトウェアが受信者のディレクトリキーを読出し、文書パッケージに対する受信者の専用ディレクトリにアクセスする；
３．クライアントソフトウェアは使用されていない印刷ライセンスを選択する。利用できる印刷ライセンスがない場合、印刷は許可されない；
４．使用されていない印刷ライセンスが利用できる場合、クライアントソフトウェアは解読のために、使用されていないライセンスをハードウェア装置に送信する。このハードウェア装置は安全保護されたメモリからライセンスキーを読出し、セッションキー１および特有のシ

ールを解読する；
５．解読のために、文書またはそのハッシュ、共通シール、時間スタンプ、および満期日がハードウェア装置に送信される。満期日がその装置内のクロックと比較される。満期日が過ぎていることを内部クロックが示した場合には、その文書は期限が切れており、印刷は許可されない。装置内でハードウェア故障が生じている場合、ユーザはハードウェア供給元に通知し、彼等にその問題を解決するように要求する；
６．装置は使用されたライセンスキーを消去する；
７．クライアントソフトウェアは、上記のステップ５の解読された文書ハッシュを使用して文書の完全性を検証し、文書をプリンタに送信するか、あるいは解読された文書をプリンタに送信する；
８．クライアントソフトウェアはプリンタと通信し、その印刷状態を監視し、文書が適当なシールを付けられて印刷される；
９．監査証跡情報が発生され、各コピーが印刷された後に受信者のＩＤキーで署名され、それによって印刷された各コピーが拒否されることのできないものになる；
１０．クライアントソフトウェアはこの装置中のＩＤリストを周期的にチェックし、期限切れのＩＤを消去する；
１１．監査証跡情報がハードウェア装置に記憶され、サーバに周期的にアップロードされる。サーバはこの監査証跡情報を予め定められた期間のあいだ維持し、この期間の終了後にその監査証跡情報は消去される。
【０１０９】［オフライン印刷制御－ソフトウェアソリューション］この状況において、印刷制御のために追加のハードウェアは必要ない。その代りに、図２０に示されているように、各受信者はソフトウェア代行業者をインストールする。
【０１１０】ソフトウェア代行業者は、修正防止、デバッグ防止等の種々の技術を使用して保護されることが好ましい。異なった印刷ライセンスに対する一連のキーはそれらの特有文書ＩＤおよび特有ＩＤキーを有し、キーデータベース（図２０）に記憶され、このキーデータベースはクライアントのローカルハードディスク上のファイルである。これらのキーは、暗号化機能のためにソフトウェア代行業者によって内部で使用される。ソフトウェア代行業者はまた各ユーザに対する専用ディレクトリを維持しており、この専用ディレクトリはユーザのＩＤキーによって保護されている。デジタル証明書を使用する場合、ユーザＩＤキーはユーザの専用（私設）キーとなることができる。
【０１１１】キーデータベースファイルは、秘密キーにより暗号化される。ソフトウェア代行業者は、秘密キーを安全保護されたメモリに記憶する。たとえば、それはハードディスク中の種々の場所にキーを分散してもよく、それによってソフトウェア代行業者が逆エンジニアリングによってキーの値を再生する試みが成功することは非常に難しくなる。
【０１１２】いくつかの状況下において、適合しないディスクユーティリティは、安全保護されたメモリを偶然的に破壊する可能性がある。この問題を解決するために安全保護メカニズムが導入される。ユーザがサーバに登録している期間中、そのサーバは再開キー対を発生する。このキー対の公開キー部分は受信者のマシン上にインストールされ、一方専用再開キーはサーバのデータベース中に保持されている。ソフトウェア代行業者は、再開公開キーにより暗号化された秘密キーのコピーを再開ファイル（図２１）として保持している。秘密キーが失われた場合、ソフトウェア代行業者はサーバと通信して、再開ファイルを使用することにより秘密キーを再生する。ソフトウェアベースのオフライン印刷制御は、上述したようにハードベースの制御の方式２と同様に動作する。
【０１１３】送信手順は次のとおりである：
１．送信者は彼等のユーザ名およびパスワードを使用して安全保護されたリンク（たとえばＳＳＬ）によって信頼できるサーバに接続される；
２．認証に成功した後、送信者は彼等の文書を以下のステップによって準備する：
（ａ）文書またはそのハッシュ、共通シール、送信に対する時間スタンプ、および文書の満期日をセッションキー１により暗号化する；
（ｂ）その文書の本文、満期日、およびステップ（ａ）の結果に対してハッシュ結果が計算される。その後、３つの部分が全てセッションキー２により暗号化され；
（ｃ）ステップ（ｂ）の結果と、受信者のＩＤと、セッションキー１と、暗号化するために使用されたセッションキー２と、その受信者が文書のＭ個のコピーを印刷するためのライセンスの数（たとえば、Ｍ）と、およびＭ個の特有のシールとをサーバに送信し、Ｍは見るだけを示すゼロであってもよい；
３．サーバが受信者の情報の正当性を検査し、図２３に示されているように、ライセンスおよびライセンスインストーラを生成する。
【０１１４】４．ライセンスは、セッションキー１と、Ｍ個のサーバ発生ランダムライセンスキーＫｅｙ１乃至ＫｅｙＭにより暗号化されたＭ個の特有のシールとを含んでいる；
５．ライセンスインストーラは、その文書に対する特有ＩＤを含んでいる。それはまた時間スタンプ（ライセンスインストーラが生成された時間）と、満期日とを含んでいる。このライセンスインストーラは受信者のＩＤキーにより暗号化される；
６．完全性チェックのために、ライセンスおよびライセンスインストーラのハッシュもまた計算される；
７．その後、サーバは図２４に示されているような文書

パッケージを生成し、これは送信者の処理した文書パッケージ［ステップ２の（ｂ）の結果］と、受信者のＩＤキーにより暗号化されたセッションキー２と、ライセンスと、およびライセンスインストーラとを含んでいる。受信者が文書を印刷することを送信者が許可していない場合、ライセンスおよびライセンスインストーラフィールドは空である；

８．サーバは、その文書を収集する準備ができたという通知を受信者に送信する。

【０１１５】受信者はこのような通知を受取って、あるいは受取らずにサーバに接続して、彼等に対する文書および、またはデータが存在しているかどうかをチェックすることができる。受信者が文書を見て印刷するための手順は：

１．受信者が彼等のユーザ名およびパスワードを使用して安全保護されたリンク（たとえば、ＳＳＬ）によって信頼できるサーバに接続され、ソフトウェア代行業者によって認証される；

２．認証の成功後、受信者は彼等自身に対するデータをサーバからダウンロードされる；

３．データを受信した後、受信者はサーバとの接続を切断するか、あるいはオンライン状態のままでいることができる；

４．クライアントソフトウェアは、ライセンスインストーラをソフトウェア代行業者に送信する；

５．ソフトウェア代行業者はＩＤキーを使用してライセンスインストーラを解読し、その完全性をチェックする。完全性チェックが失敗であった場合には、受信者はサーバに通知し、その問題を解決するようにサーバに要求しなければならない；

６．ソフトウェア代行業者は、キーデータベースに保管されたＩＤのリストにより文書ＩＤをチェックする；

７．一致するものが１つもない場合、システムクロックに対して時間スタンプと満期日がチェックされる。満期日の期限が切れていた場合、ライセンスはインストールされることができない；

８．全てのチェック手順が成功的に完了すると、ライセンスキーがキーデータベースにインストールされ、ＩＤがＩＤリストに記憶される；

９．解読のために、クライアントソフトウェアは暗号化されたセッションキー２をソフトウェア代行業者に送信する。ソフトウェア代行業者は、解読されたセッションキー２をクライアントソフトウェアに返信し、その後このクライアントソフトウェアが文書を解読し、その完全性をチェックする。完全性チェックが失敗であった場合、受信者はサーバに通知し、この問題を解決するようにサーバに要求しなければならない。そうでない場合は、文書パッケージは受信者の専用ディレクトリに記憶される。

【０１１６】受信者が文書を見るための手順は次のとおりである：

１．受信者が彼等のユーザ名とパスワードによりクライアントソフトウェアにログオンし、ソフトウェア代行業者によって認証される；

２．認証の成功後、ソフトウェア代行業者はその文書パッケージに対する受信者の専用ディレクトリにアクセスする；

３．満期日がシステムクロックと比較される。満期日が過ぎていることをシステムクロックが示した場合、その文書は期限切れであり、それを見ることは許されない；

４．文書が期限切れでない場合、受信者はその文書を見ることができる。

【０１１７】受信者が文書を印刷するために：

１．受信者が彼等のユーザ名とパスワードによりクライアントソフトウェアにログオンし、ソフトウェア代行業者によって認証される；

２．認証の成功後、ソフトウェア代行業者がその文書パッケージに対する受信者の専用ディレクトリにアクセスする；

３．クライアントソフトウェアは使用されていない印刷ライセンスを選択し、それをソフトウェア代行業者に送信する。印刷ライセンスが１つも残っていない場合、印刷は許可されない；

４．使用されていない印刷ライセンスがある場合、ソフトウェア代行業者はそのライセンスからのセッションキー１と特有のシールを解読する；

５．文書またはそのハッシュ、共通シール、時間スタンプ、および満期日がセッションキー１を使用して解読される。満期日がシステムクロックと比較される。満期日が過ぎていることをシステムクロックが示した場合、その文書は期限切れであり、印刷は許可されない。

【０１１８】６．クライアントソフトウェアは上記のステップ５からの解読された文書ハッシュを使用して文書の完全性を検証し、その文書をプリンタに送信するか、あるいは解読された文書をプリンタに送信する；

７．クライアントソフトウェアはプリンタと通信し、印刷プロセスの状態を監視し、その文書が適当なシールを付けて印刷される；

８．監査証跡情報が発生され、各コピーが印刷された後に受信者のＩＤキーで署名され、それによって印刷された各コピーが拒否されることのできないものになる；

９．クライアントソフトウェアは、キーデータベース中のＩＤリストを周期的にチェックし、期限切れのＩＤを除去する；

１０．監査証跡情報がキーデータベースに記憶され、サーバに周期的にアップロードされる。サーバはこの監査証跡情報を予め定められた期間中維持し、この期間の終了後それは消去される；

１１．クライアントソフトウェアは新しい秘密キーを発生し、そのキーデータベースを再度暗号化する；

12．クライアントソフトウェアは、新しい秘密キーを再開公開キーにより暗号化することによって新しいキー再開ファイルを生成する。

【0119】上記の説明において、対称キーまたは公開キーのどちらでも都合に応じて使用されることができる。いずれの場合も、対称キーおよび公開キーが共に適応可能である。予め定められた期間はユーザまたはサーバによって、あるいはその両者間の取決めによって設定されることができる。

【0120】また、送信者およびサーバは1つでもよい。たとえば、nの発行オーソリティは送信者およびサーバであってよく、この場合そのサーバは両者の機能を行う。

【0121】認められるように、本発明は、ネットワークによって送信された認証された文書の遠隔的な印刷に関する。これによって、認証された紙文書の高価で時間のかかる物理的な配達が回避される。本発明の適用が非常に有効な分野が存在する。その1つは、安全保護された印刷工場である。彼等は、信頼できる権限の与えられた代行業者である。現金手形および銀行小切手のような法的に認証された文書は、特殊のプリンタ、特殊のインク、特殊の紙およびその他の特殊な材料を使用して印刷されることができる。印刷プロセスおよび印刷材料は共に厳しく制御される。他のものは署名された文書であり、この場合は権限を有する者が彼等の署名および、シールによりその文書を初期化する。両方の場合において、文書に認証を付加する署名および特殊印刷材料は、権限を与えられた人物または代行業者によって完全に制御される。

【0122】たとえば、送信者およびサーバが1つの場合、サーバは、たとえば、郵便局のような発行権限を有する部署の一部分であることができ、また制御された印刷は郵便切手の印刷であることができる。別の例は、オーソリティがチケット取次販売所であり、制御された印刷がコンサートのようなイベント、スポーツイベント、映画等のチケットの印刷の場合である。いくつかの国では、内国税収入サービスまたはその等価な機関が、商売をしている者に領収書番号を発行し、正式な領収書が代金の受取りごとに発行されなければならない。これによって彼等は商店が受取った代金をチェックし続けることができる。印刷の制御は領収書番号の印刷であることができる。

【0123】本発明はまた、文書の信頼できる印刷または送信が必要とされる場合に使用できる。この中には税金明細記入請求書または領収書が含まれてもよく、その場合以下のステップが含まれる可能性がある：

（a）関連政府管轄局が秘密の安全性が保護されたハードウェア装置を各事業主に供給する；

（b）その管轄局が標準の税金明細記入請求書および、または領収書形式とライセンスキーとをその事業主に供給する；

（c）事業主はそのハードウェア装置を使用して税金明細記入請求書および、または領収書を発生し、その後これら請求書および、または領収書をその顧客に電子的にまたはハードコピーで送る。電子的に送信された場合、ハードウェア装置は、それがハードコピーの印刷に対して行うのと同じ方法で送信プロセスを制御する；

（d）ハードウェア装置は監査証跡情報を生成し、各領収書および明細記入請求書の総額を含む全ての必要なデータを記録する；

（e）監査証跡情報は、ライセンスキーがトップアップされたときに管轄局に送信される。それによって、管轄局は監査証跡から得られた情報に基づいて各事業主が支払うべき税金を決定することができる。

【0124】上記の説明では、本発明の好ましい実施形態が記載されているが、当業者は、本発明の技術的範囲を逸脱することなく多数の詳細な変形または修正が可能であることを理解するであろう。

【0125】本発明は、開示されている個々の特徴のそれぞれ、およびこれらの各特徴の可能性のある全ての置換および組合せに及んでいる。

【0126】

【図面の簡単な説明】

【図1】文書伝送および印刷システムのブロック図。

【図2】信頼できる文書の構造の概略図。

【図3A】ＰＪＬ言語を使用するプリンタ制御のフロー図。

【図3B】ＰＪＬ言語を使用するプリンタ制御のフロー図。

【図4】オフライン印刷用のハードウェア装置のブロック図。

【図5】第1のオフライン印刷方式のブロック図。

【図6】図5の方式において使用される文書データフォーマットの概略図。

【図7】トップアップキーセットの生成を示す概略図。

【図8】図7のトップアップ手順のフロー図。

【図9】第2のオフライン印刷方式のブロック図。

【図10】図9の方式において使用される文書データフォーマットの概略図。

【図11】図9および10の方式で使用されるライセンスおよびライセンスインストーラデータフォーマットの概略図。

【図12】第2のオフライン印刷用ハードウェア装置のブロック図。

【図13】第3のオフライン印刷方式のブロック図。

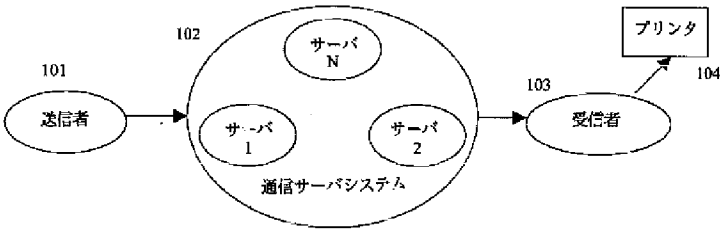
【図14】図13の方式において使用される文書データフォーマットの概略図。

【図15】トップアップキーセットの生成を示す概略図。

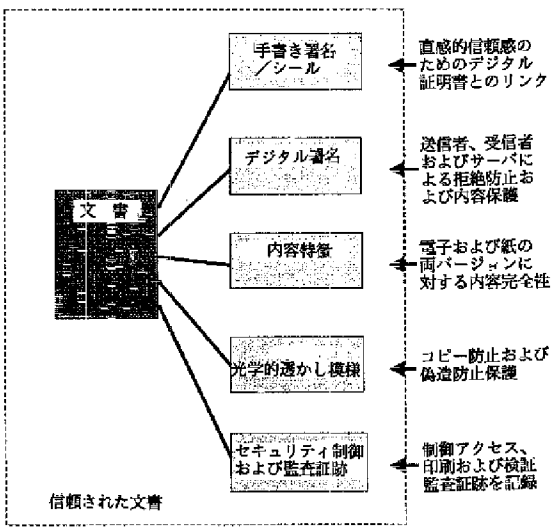
【図16】図15のトップアップ手順のフロー図。

【図１７】第４のオフライン印刷方式のブロック図。
【図１８】図１７の方式において使用される文書データフォーマットの概略図。
【図１９】図１７および１８の方式で使用されるライセンスおよびライセンスインストーラデータフォーマットの概略図。
【図２０】ソフトウェアベースのオフライン印刷用のキーデータベースの概略図。
【図２１】ソフトウェアベースのオフライン印刷用のキーレスキューファイルの概略図。
【図２２】ソフトウェアベースのオフライン印刷方式のブロック図。
【図２３】ソフトウェアベースのオフライン印刷方式で使用されるライセンスおよびライセンスインストーラデータフォーマットの概略図。
【図２４】ソフトウェアベースのオフライン印刷方式で使用される文書データフォーマットの概略図。

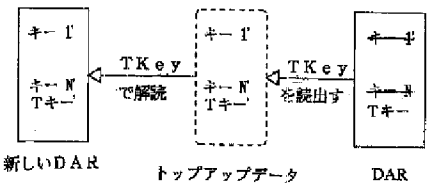
【図１】



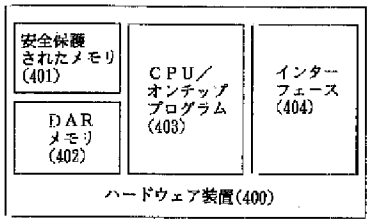

【図２】



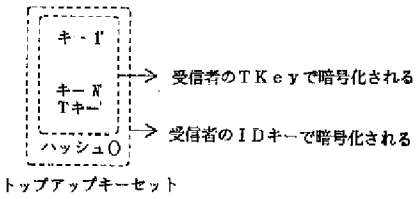

【図８】



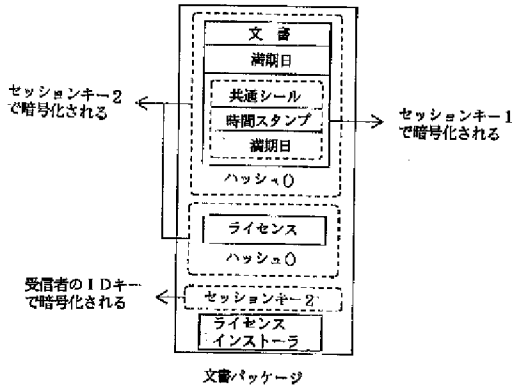

【図４】



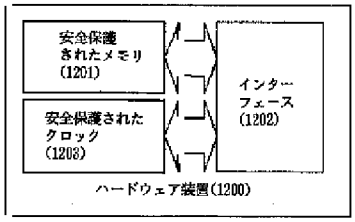

【図７】



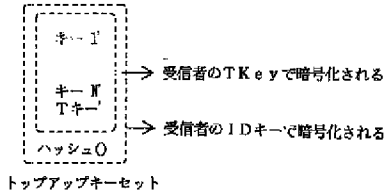

【図１０】



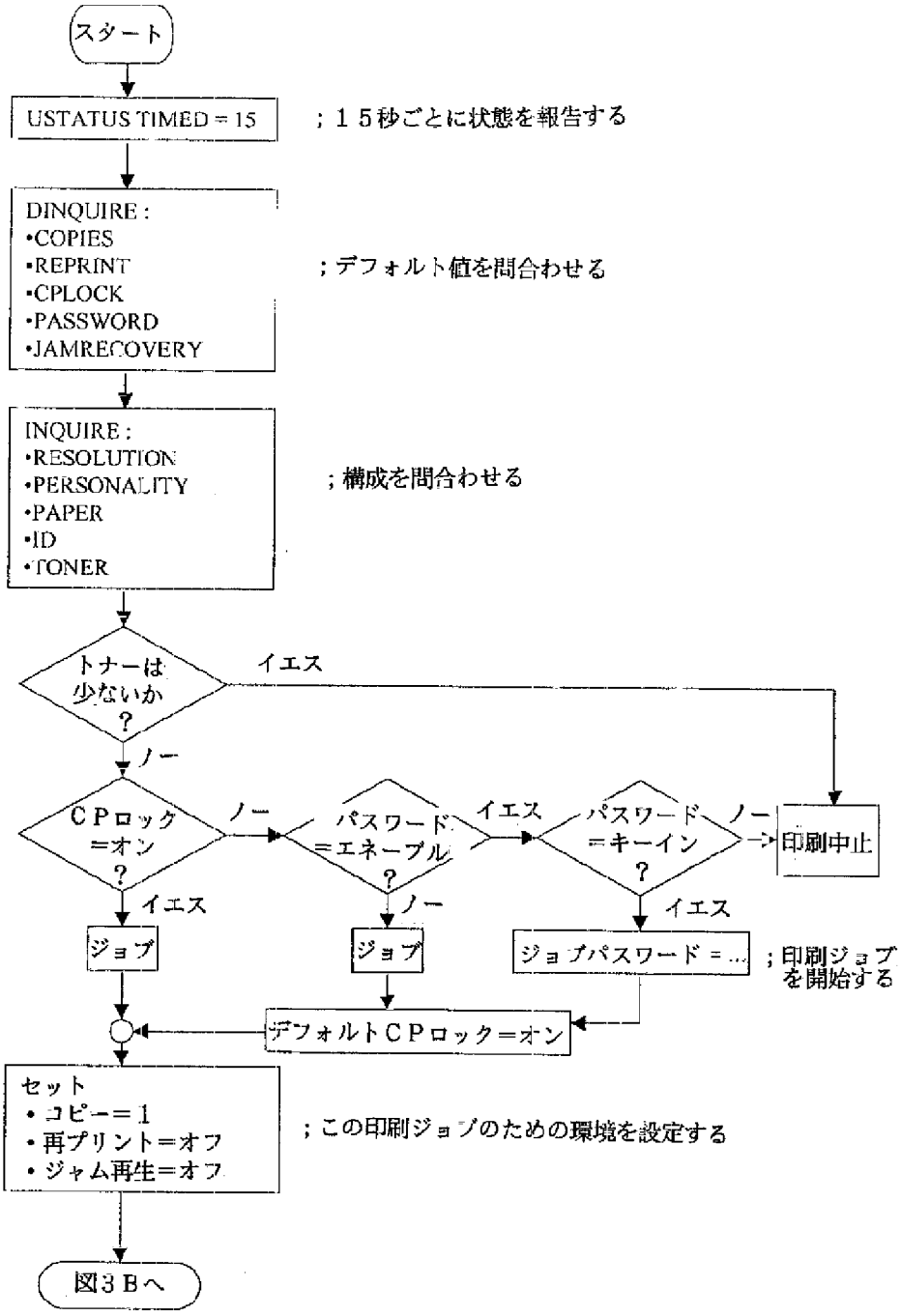

【図１２】



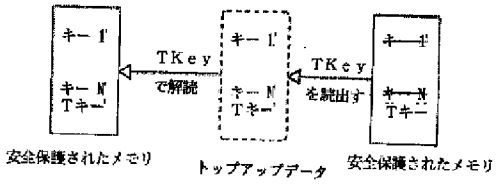

【図１５】



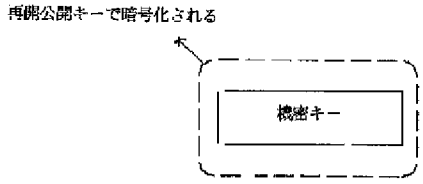
【図３Ａ】


スタート
USTATUS TIMED = 15
；１５秒ごとに状態を報告する
DINQUIRE :
•COPIES
•REPRINT
•CPLOCK
•PASSWORD
•JAMRECOVERY
；デフォルト値を問合わせる
INQUIRE :
•RESOLUTION
•PERSONALITY
•PAPER
•ID
•TONER
；構成を問合わせる
トナーは少ないか？
イエス
ノー
ＣＰロック＝オン？
ノー
パスワード＝エネーブル？
イエス
パスワード＝キーイン？
ノー
印刷中止
イエス
ノー
イエス
ジョブ
ジョブ
ジョブパスワード＝...
；印刷ジョブを開始する
デフォルトＣＰロック＝オン
セット
• コピー＝１
• 再プリント＝オフ
• ジャム再生＝オフ
；この印刷ジョブのための環境を設定する
図３Ｂへ

【図１６】


キー I'
キー N
Tキー
TKey
で解読
キー I'
キー N
Tキー
TKey
を読出す
キー I'
キー N
Tキー
安全保護されたメモリ
トップアップデータ
安全保護されたメモリ

【図２１】


再開公開キーで暗号化される
機密キー

【図３Ｂ】

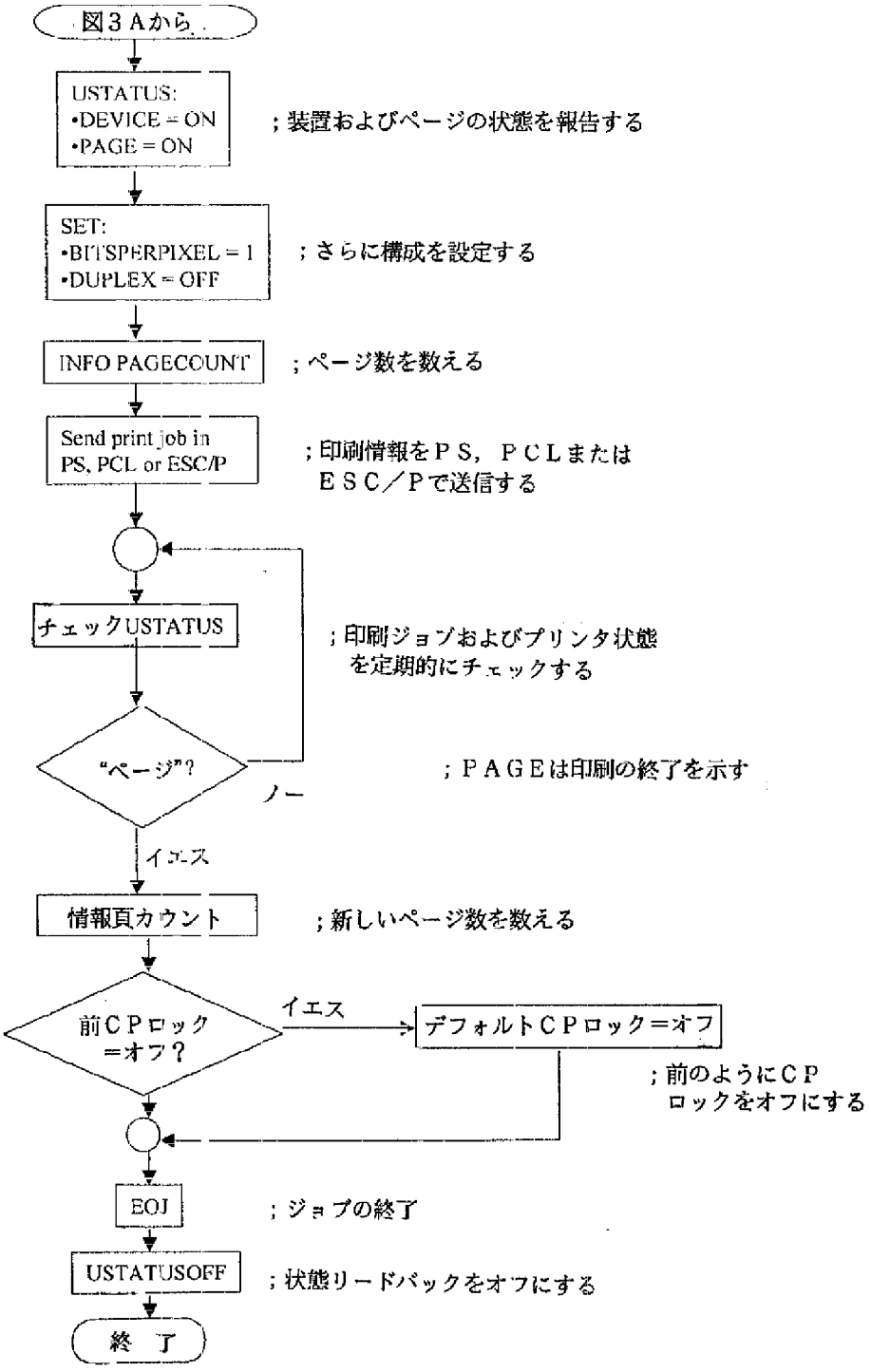
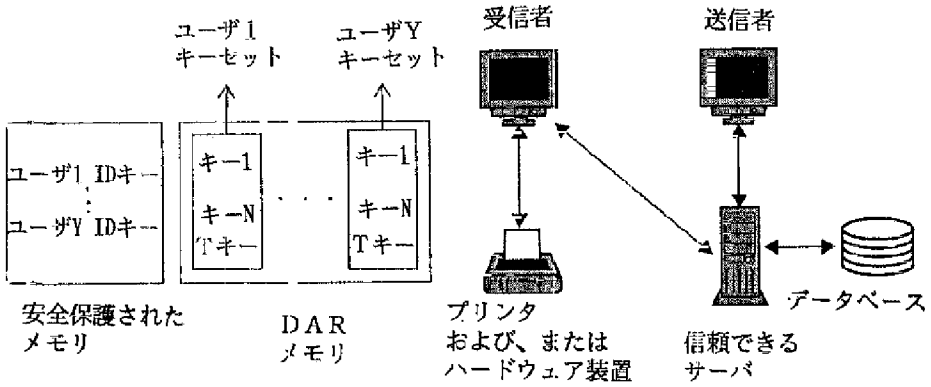
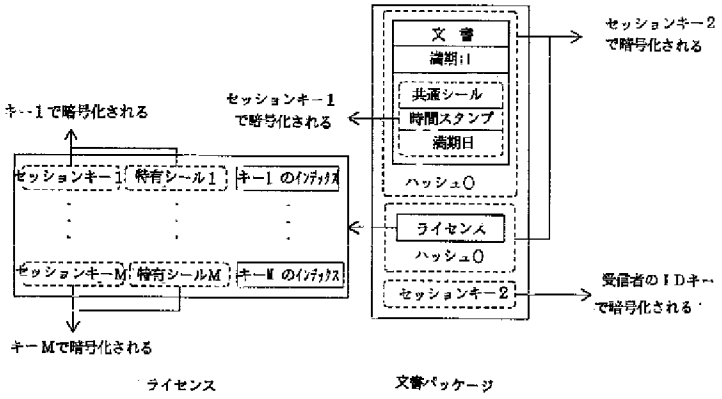


図３Ａから
USTATUS:
•DEVICE = ON
•PAGE = ON
；装置およびページの状態を報告する
SET:
•BITSPERPIXEL = 1
•DUPLEX = OFF
；さらに構成を設定する
INFO PAGECOUNT
；ページ数を数える
Send print job in
PS, PCL or ESC/P
；印刷情報をＰＳ，ＰＣＬまたは
ＥＳＣ／Ｐで送信する
チェックUSTATUS
；印刷ジョブおよびプリンタ状態
を定期的にチェックする
“ページ”?
；ＰＡＧＥは印刷の終了を示す
ノー
イエス
情報頁カウント
；新しいページ数を数える
前ＣＰロック
＝オフ？
イエス
デフォルトＣＰロック＝オフ
；前のようにＣＰ
ロックをオフにする
EOJ
；ジョブの終了
USTATUSOFF
；状態リードバックをオフにする
終　了

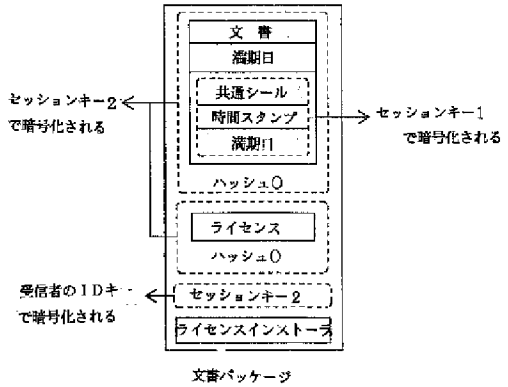
【図5】


ユーザ1
キーセット
ユーザY
キーセット
受信者
送信者
ユーザ1 IDキー
ユーザY IDキー
キー1
キーN
Tキー
キー1
キーN
Tキー
データベース
安全保護された
メモリ
DAR
メモリ
プリンタ
および、または
ハードウェア装置
信頼できる
サーバ

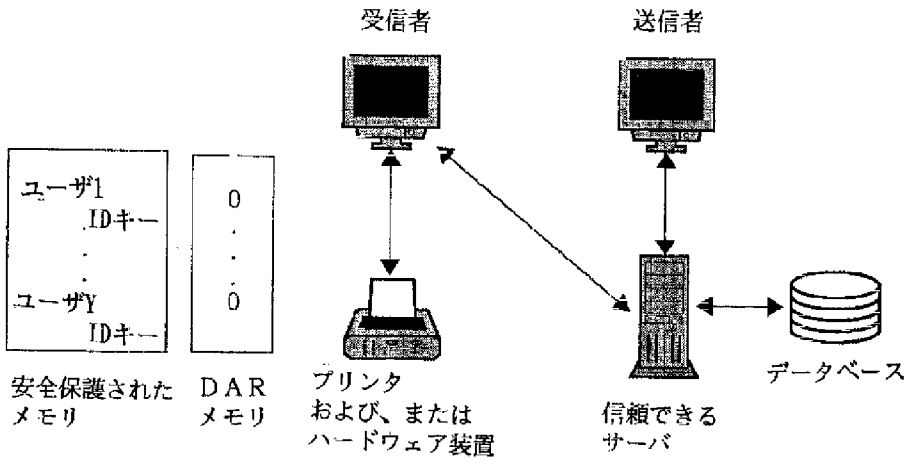
【図6】


文書
満期日
共通シール
時間スタンプ
満期日
ハッシュ0
ライセンス
ハッシュ0
セッションキー2
セッションキー2
で暗号化される
セッションキー1
で暗号化される
キー1で暗号化される
セッションキー1
特有シール1
キー1 のインデックス
セッションキーM
特有シールM
キーM のインデックス
キーMで暗号化される
受信者のIDキー
で暗号化される
ライセンス
文書パッケージ

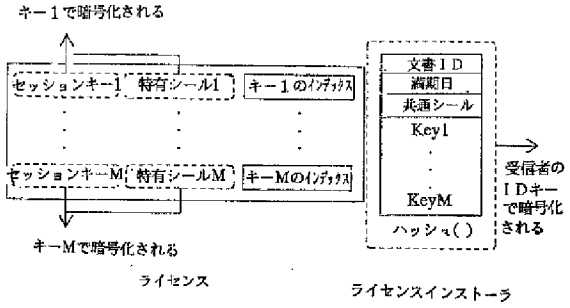
【図18】


文書
満期日
共通シール
時間スタンプ
満期日
ハッシュ0
ライセンス
ハッシュ0
セッションキー2
セッションキー2
で暗号化される
セッションキー1
で暗号化される
受信者のIDキー
で暗号化される
ライセンスインストール
文書パッケージ

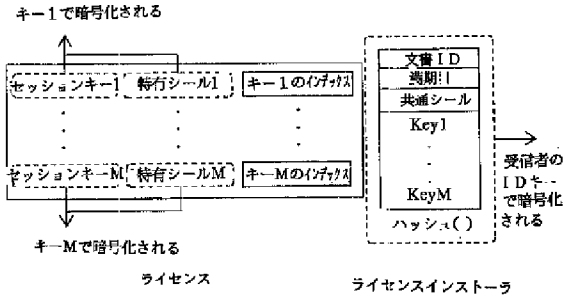
【図9】


受信者
送信者
ユーザ1
IDキー
ユーザY
IDキー
0
0
データベース
安全保護された
メモリ
DAR
メモリ
プリンタ
および、または
ハードウェア装置
信頼できる
サーバ

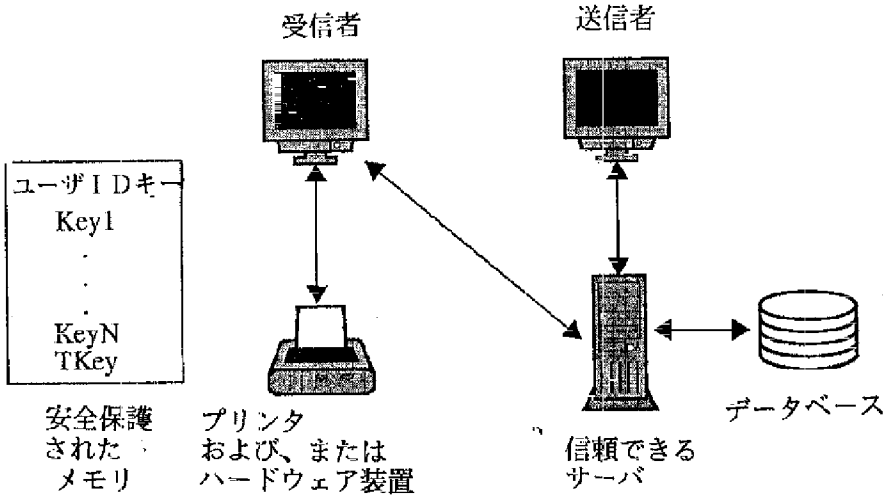
【図11】



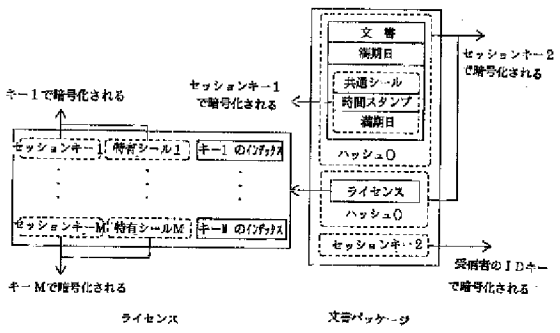

【図19】



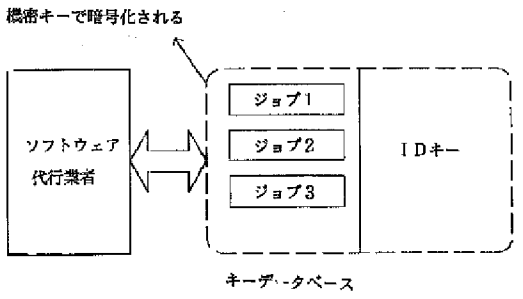

【図13】



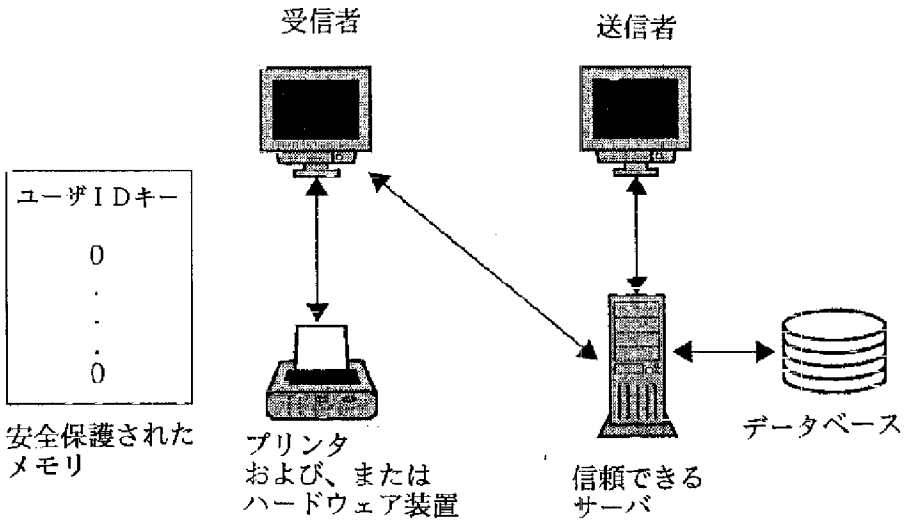

【図14】



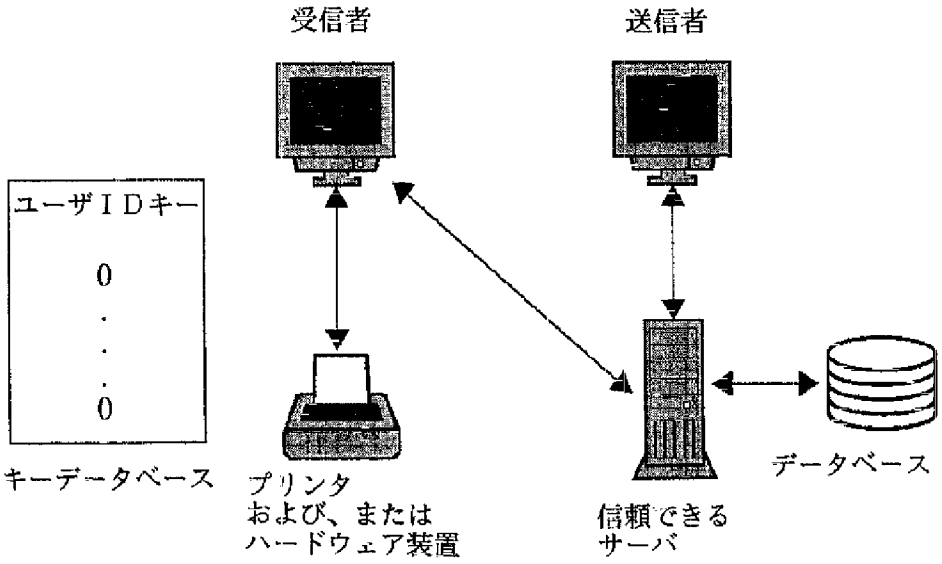

【図20】



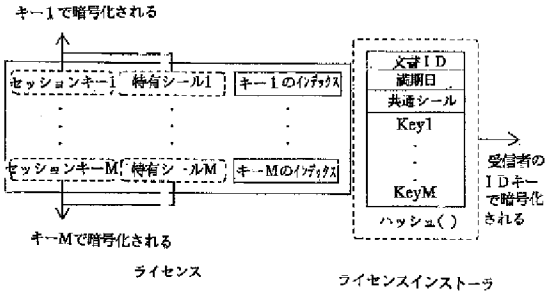
【図１７】



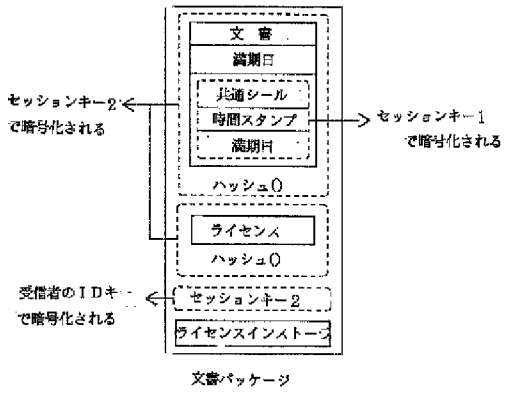

【図２２】




【図２３】




【図２４】



フロントページの続き

| (51)Int.Cl.[7] | | 識別記号 |
|---|---|---|
| Ｇ０６Ｆ | 12/14 | ３２０ |
| | 15/00 | ３３０ |
| Ｇ０９Ｃ | 1/00 | ６４０ |
| Ｈ０４Ｎ | 1/44 | |

| ＦＩ | | （参考） |
|---|---|---|
| Ｇ０６Ｆ | 12/14 | ３２０Ｆ　５Ｃ０７５ |
| | 15/00 | ３３０Ａ　５Ｊ１０４ |
| | | ３３０Ｂ |
| Ｇ０９Ｃ | 1/00 | ６４０Ｂ |
| Ｈ０４Ｎ | 1/44 | |
| Ｂ４１Ｊ | 29/00 | Ｚ |

(72)発明者　バオシ・ツゥ
シンガポール国、130035　ドーバー・ロード、ナンバー　13－163、ビーエルケー35
(72)発明者　クンイン・ツゥ
シンガポール国、650243　ブキット・バトック・イースト・アベニュー　３、ナンバー　05－38、ビーエルケー　243
(72)発明者　シェン・ファン
シンガポール国、600403　パンダン・ガーデンズ、ナンバー　08－16、ビーエルケー403

Ｆターム(参考)　2C061 AP01 CL08 HJ10 HN16 HQ17
2C087 AA13 AB05 BD02 DA14
5B017 AA06 AA07 BA05 BA07 BB10 CA16
5B021 AA01 EE04
5B085 AE02 AE03 BA07 BC01 BG07
5C075 AB90 CA14 EE02 EE03 FF90
5J104 AA09 AA14 LA03 NA02 NA05 PA07 PA14